Gateway™

User Guide

Gateway 7001 Series Access Point

Contents

Chapter 1

Introduction

- Features and benefits
- Networking
- Maintainability
- Default settings and supported administrator/client platforms

Overview of the Gateway 7001 Series of self-managed APs

The Gateway 7001 Series of self-managed APs (access points) provide continuous, high-speed access between your wireless and Ethernet devices. They are advanced, turnkey solutions for wireless networking in small and medium-sized businesses. The Gateway 7001 Series enables zero-administration wireless local area network (WLAN) deployment while providing state-of-the-art wireless networking features.

The Gateway 7001 AP is available as a single band access point (Gateway 7001 802.11 G Wireless Access Point) and a dual band access point (Gateway 7001 802.11 A+G Wireless Access Point).

The single band access point can broadcast in either IEEE 802.11b or IEEE 802.11g mode.

The dual band access point is capable of broadcasting in two different IEEE 802.11 modes simultaneously.

- Radio One can broadcast in IEEE 802.11b or IEEE 802.11g modes.
- Radio Two can broadcast in IEEE 802.11a or IEEE 802.11a Turbo modes.

The Gateway 7001 AP software solution emphasizes security, ease-of-administration and industry standards—providing a standalone and fully secured wireless network without the need for additional management applications such as legacy authentication server software.

The following sections list features and benefits of the Gateway 7001 Series self-managed APs, and tell you what's next when you're ready to get started.

Features and benefits

IEEE standards support and Wi-Fi compliance

- Support for IEEE 802.11a, 802.11b, and 802.11g wireless networking standards (depending on model)
- Provides bandwidth of up to 54 Mbps for 802.11a or 802.11g (11 Mbps for 802.11b, 108 Mbps for 802.11a Turbo)
- Wi-Fi certified

Wireless features

- Auto channel selection at startup
- Transmit power adjustment
- Wireless Distribution System (WDS) for connecting multiple access points wirelessly. Extends your network with less cabling and provides a seamless experience for roaming clients.
- Virtual Local Area Network (VLAN) support
- Under-the-hood support for multiple SSIDs (network names) and multiple BSSIDs (basic service set IDs) on the same access point

Security features

- Inhibit SSID Broadcast
- Ignore SSID Broadcast
- Link integrity monitoring
- Link integrity checking
- Weak IV avoidance
- Wireless Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- Advanced Encryption Standard (AES)
- User-based access control with local authentication server
- Local user database and user lifecycle management
- MAC address filtering

Out-of-the-Box guest interface

- Unique network name (SSID) for the Guest interface
- Captive portal to guide guests to customized, guest-only Web page
- VLAN and dual Ethernet options

Clustering and auto-management

- Automatic setup with Kickstart.
- Provisioning and plug-and-play through automatic clustering and cluster rendezvous.

  The administrator can specify how new access points should be configured before they are added to the network. When new access points are added, they can automatically rendezvous with the cluster, and securely download the correct configuration. The process does not require manual intervention, but is under the control of the administrator.

- Single universal view of clustered access points and cluster configuration settings.

  Configuration for all access points in a cluster can be managed from a single interface. Changes to common parameters are automatically reflected in all members of the cluster.

- Self-managed access points with automatic configuration synchronization.

  The access points in a cluster periodically check that the cluster configuration is consistent, and check for the presence and availability of the other members of the cluster. The administrator can monitor this information through the user interface.

- Enhanced local authentication using 802.1x without additional IT setup.

  A cluster can maintain a user authentication server and database stored on the access points. This eliminates the need to install, configure, and maintain a RADIUS infrastructure, and simplifies the administrative task of deploying a secure wireless network.

- Hardware watchdog.

Networking

- Dynamic Host Configuration Protocol (DHCP) support for dynamically assigning network configuration information to systems on the LAN

Maintainability

- Status, monitoring, and tracking views of the network including session monitoring, client associations, transmit/receive statistics, and event log
- Reset configuration option
- Firmware upgrade

Default settings and supported administrator/client platforms

Before you plug in and boot a new access point, review the following sections for a quick check of required hardware components, software, client configurations, and compatibility issues. Make sure you have everything you need ready to go for a successful launch and test of your new (or extended) wireless network.

- Gateway 7001 Series self-managed AP
- Administrator's computer
- Wireless client computers
- Understanding of DHCP IP addressing for access points and wireless clients

Gateway 7001 Series self-managed AP

The Gateway 7001 Series self-managed AP is a wireless communications hub for devices on your network. It provides continuous, high-speed access between your wireless and Ethernet devices in IEEE 802.11a, 802.11b, 802.11g, or 802.11a Turbo modes (depending on the model).

The Gateway 7001 Series self-managed AP offers an out-of-the-box Guest Interface feature that lets you configure access points for controlled guest access of the wireless network. This can be accomplished either by using Virtual LANs or by creating physically separate network connections on the same access point. To support physically separate network connections, the Gateway 7001 Series self-managed AP ships with an extra network port to be used for a dedicated guest network. (For more information on the guest interface, see "Advanced Configuration" on page 67, and "Setting up connections for a guest network" on page 19.)

Default settings for the Gateway 7001 Series self-managed AP

Option	Default Settings	Related Information
System Name	Gateway-AP	"Setting the DNS name" on page 69
User Name	admin The user name is read-only. It cannot be modified.	

Option	Default Settings	Related Information
Password	admin	“Providing administrator password and wireless network name” on page 32 “Configuring security settings on wireless clients” on page 121
Network Name (SSID)	“Gateway 7001 AP Network” for the Internal interface “Gateway 7001 AP Guest Network” for the Guest interface	“Reviewing and describing the access point” on page 31 “Configuring internal LAN wireless settings” on page 76 “Configuring guest network wireless settings” on page 76
Network Time Protocol (NTP)	None	“Enabling a network time protocol server” on page 78
IP Address	192.168.1.1 The default IP address is used if you do not use a Dynamic Host Configuration Protocol (DHCP) server. You can assign a new static IP address through the Administration Web pages. If you have a DHCP server on the network, then an IP address will be dynamically assigned by the server at AP startup.	“Understanding dynamic and static IP addressing” on page 12
Connection Type	Dynamic Host Configuration Protocol (DHCP) If you do not have a DHCP server on the Internal network and do not plan to use one, the first thing you must do after bringing up the access point is to change the Connection Type from “DHCP” to “Static IP”. The Guest network must have a DHCP server.	“Understanding dynamic and static IP addressing” on page 12 For information on how to re-configure the Connection Type, see “Configuring Internal interface Ethernet settings” on page 71.
Subnet Mask	255.255.255.0	
Radio	On	“Configuring radio settings” on page 104

Option	Default Settings	Related Information
IEEE 802.11 Mode	802.11g pr 802.11a+g	“Configuring radio settings” on page 104
802.11g Channel	Auto	“Configuring radio settings” on page 104
Beacon Interval	100	“Configuring radio settings” on page 104
DTIM Period	2	“Configuring radio settings” on page 104
Fragmentation Threshold	2346	“Configuring radio settings” on page 104
ATS Threshold	2347	“Configuring radio settings” on page 104
MAX Stations	2007	“Configuring radio settings” on page 104
Transmit Power	100 Percent (of certified level)	“Configuring radio settings” on page 104
Rate Sets Supported (Mbps)	IEEE 802.11a: 54, 48, 36, 24, 18, 12, 9, 6 IEEE 802.11g: 54, 48, 36, 24, 18, 12, 9, 6, 5.5, 2, 1 IEEE 802.11b: 11, 5.5, 2, 1 Atheros Turbo 5 GHz: 108, 96, 72, 48, 36, 24, 18, 12	“Configuring radio settings” on page 104
Rate Sets (Basic/Advertised)	IEEE 802.11a: 24, 12, 6 IEEE 802.11g: 11, 5.5, 2, 1 IEEE 802.11b: 2, 1 Atheros Turbo 5 GHz: 48, 24, 12	“Configuring radio settings” on page 104
Broadcast SSID	Allow	“Broadcast SSID and Security Mode” on page 88
Security Mode	None (plain text)	“Broadcast SSID and Security Mode” on page 88
Authentication Type	None	

Option	Default Settings	Related Information
MAC Filtering	Allow any station unless in list	“Controlling access by MAC address filtering” on page 110
Guest Login	Disabled	“Advanced Configuration” on page 67
Guest Welcome Screen Text	Thank you for using wireless Guest Access as provided by this Gateway 7001 Series wireless access point. When clicking “Accept” below, you will gain access to a wireless network which will allow you complete access to the Internet but is external to the corporate network. This network is not configured to provide any level of wireless security.	“Advanced Configuration” on page 67
WDS Settings	None	“Configuring a Wireless Distribution System (WDS)” on page 112

What the access point does not provide

The Gateway 7001 Series self-managed AP is not designed to function as a gateway to the Internet. To connect your LAN to other LANs or the Internet, you need a gateway device, such as a router or a switch.

Administrator's computer

Configuration and administration of the Gateway 7001 Series self-managed AP is accomplished with the KickStart utility (which you run from the CD) and through a Web-based user interface (UI). The following table describes the minimum requirements for the administrator's computer.

Required Software or Component	Description
Ethernet Connection to the First Access Point	The computer used to configure the first access point with KickStart must have an Ethernet network connection to the access point.
Wireless Connection to the Network	After initial configuration and launch of the first access points on your new wireless network, you can make subsequent configuration changes through the Administration Web pages using a wireless connection to the "Internal" network. For wireless connection to the access point, your administration device will need Wi-Fi capability similar to that of any wireless client: • Portable or built-in Wi-Fi client adapter that supports one or more of the IEEE 802.11 modes in which you plan to run the access point. (IEEE 802.11a, 802.11b, 802.11g, and 802.11a Turbo modes are supported, depending on model.) • Wireless client software such as Microsoft Windows XP or Funk Odyssey wireless client configured to associate with the Gateway 7001 Series access point. For more details on Wi-Fi client setup, see "Wireless client computers" on page 11
Web Browser / Operating System	Configuration and administration of the Gateway 7001 Series self-managed AP is provided through a Web-based user interface hosted on the access point. We recommend using one of the following supported Web browsers to access the access point Administration Web pages: • Microsoft Internet Explorer version 5.5 or 6.x (with up-to-date patch level for either major version) on Microsoft Windows XP or Microsoft Windows 2000 • Netscape Mozilla on Redhat Linux version 2.4 The administration Web browser must have JavaScript enabled to support the interactive features of the administration interface. It must also support HTTP uploads to use the firmware upgrade feature.

Required Software or Component	Description
KickStart Wizard on CD	You can run the KickStart CD on any laptop or computer that is connected to the access point (through Wired or Wireless connection). It detects Gateway 7001 Series self-managed APs on the network. The wizard steps you through initial configuration of new access points, and provides a link to the Administration Web pages where you finish up the basic setup process in a step-by-step mode and launch the network. For more about using KickStart, see “Running KickStart to find access points and assign IP addresses” on page 20
CD Drive	The administrator’s computer must have a CD drive to run the KickStart CD.
Security Settings	Make sure that security is disabled on the wireless client used to initially configure the access point.

Wireless client computers

The Gateway 7001 Series self-managed AP provides wireless access to any client with a correctly configured Wi-Fi client adapter for the 802.11 mode in which the access point is running.

Multiple client operating systems are supported. Clients can be laptops or desktops, personal digital assistants (PDAs), or any other hand-held, portable or stationary device equipped with a Wi-Fi adapter and supporting drivers.

In order to connect to the access point, wireless clients need the following software and hardware.

Required Component	Description
Wi-Fi Client Adapter	Portable or built-in Wi-Fi client adapter that supports one or more of the IEEE 802.11 modes in which you plan to run the access point. (IEEE 802.11a, 802.11b, 802.11g, and 802.11a Turbo modes are supported, depending on model.) Wi-Fi client adapters vary considerably. The adapter can be a PC card built in to the client device, a portable PCMCIA or PCI card (types of NICs), or an external device such as a USB or Ethernet adapter that you connect to the client by means of a cable. The access point supports 802.11a/b/g modes (depending on model), but you will probably make a decision during network design phase as to which mode to use. The fundamental requirement for clients is that they all have configured adapters that match the 802.11 mode for which your access point(s) is configured.
Wireless Client Software	Client software such as Microsoft Windows XP or Funk Odyssey wireless client configured to associate with the Gateway 7001 Series access point.
Client Security Settings	Security should be disabled on the client used to do initial configuration of the access point. If the Security mode on the access point is set to anything other than plain text, wireless clients will need to set a profile to the authentication mode used by the access point and provide a valid user name and password, certificate, or similar user identity proof. Security modes are Static WEP, IEEE 802.1x, WPA with RADIUS server, and WPA-PSK. For information on configuring security on the access point, see “Configuring network security” on page 80.

Understanding dynamic and static IP addressing

Gateway 7001 Series self-managed APs are built to auto-configure, with very little setup required for the first access point and no configuration required for additional access points subsequently joining a preconfigured cluster.

How does the access point obtain an IP address at startup?

When you deploy the access point, it looks for a network DHCP server and, if it finds one, obtains an IP Address from the DHCP server. If no DHCP server is found on the network, the AP will continue to use its default Static IP Address (192.168.1.1) until you re-assign it a new static IP address (and specify a static IP addressing policy) or until a DHCP server is brought online.

Important

If you configure both an Internal and Guest network and plan to use a dynamic addressing policy for both, separate DHCP servers must be running on each network.

A DHCP server is a requirement for the Guest network.

When you run KickStart, it discovers the Gateway 7001 Series self-managed APs on the network and lists their IP addresses and MAC addresses. KickStart also provides a link to the administration Web pages of each access point using the IP address in the URL. (For more information about the KickStart utility, see "Running KickStart to find access points and assign IP addresses" on page 20.)

Dynamic IP addressing

The Gateway 7001 Series self-managed AP generally expects that a DHCP server is running on the network where the AP is deployed. Most home and small business networks already have DHCP service provided either through a gateway device or a centralized server. However, if no DHCP server is present on the Internal network, the AP will use the default Static IP Address for first time startup.

Similarly, wireless clients and other network devices (such as printers) will receive their IP addresses from the DHCP server, if there is one. If no DHCP server is present on the network, you must manually assign static IP addresses to your wireless clients and other network devices.

The Guest network must have a DHCP server.

Static IP addressing

The Gateway 7001 Series self-managed AP ships with a default Static IP Address of 192.168.1.1. (See the default settings for the AP in "Gateway 7001 Series self-managed AP" on page 5.) If no DHCP server is found on the network, the AP retains this static IP address at first-time startup.

After AP startup, you have the option of specifying a static IP addressing policy on Gateway 7001 Series self-managed APs and assigning static IP addresses to APs on the internal network through the access point Administration Web pages. (See information about the **Connection Type** box and related boxes in "Configuring Internal interface Ethernet settings" on page 71.)

Important

If you do not have a DHCP server on the Internal network and do not plan to use one, the first thing you must do after adding the access point is change the Connection Type from DHCP to Static IP. You can either assign a new Static IP address to the AP or continue using the default address. We recommend assigning a new Static IP address so that if later you add another Gateway 7001 Series self-managed AP on the same network, the IP address for each AP will be unique.

Recovering an IP Address

If you experience trouble communicating with the access point, you can recover a static IP address by resetting the AP configuration to the factory defaults (see "Resetting the configuration" on page 166), or you can get a dynamically assigned address by connecting the AP to a network that has DHCP.

Chapter 2

Quick Setup

- Unpacking the access point
- Connecting the access point to network and power
- Turning on the access point
- Running KickStart to find access points and assign IP addresses
- Configuring basic settings and starting the wireless network

Setting up the access point

Setting up and deploying one or more Gateway 7001 Series self-managed APs is in effect creating and launching a *wireless network*. The KickStart Wizard and corresponding Basic Settings Administration Web page simplify this process. Here is a step-by-step guide to setting up your Gateway 7001 Series self-managed APs and the resulting wireless network. Have the KickStart CD handy, and familiarize yourself with the "Default settings and supported administrator/client platforms" on page 5 if you have not already.

Unpacking the access point

Unpack the Access Point (AP) and familiarize yourself with its hardware ports, associated cables, and accessories.

Access point hardware and ports

The access point includes:

- Ethernet ports for connection to the Local Area Network (LAN) through Ethernet network cable
- Power over Ethernet (POE) and power adapter

What's inside the access point?

An access point is a single-purpose computer designed to function as a wireless hub. Inside the access point is a Wi-Fi radio system, a microprocessor, and sometimes a mini-PC card. The access point boots from FlashROM that contains firmware with the configurable, runtime features summarized in "Overview of the Gateway 7001 Series of self-managed APs" on page 2.

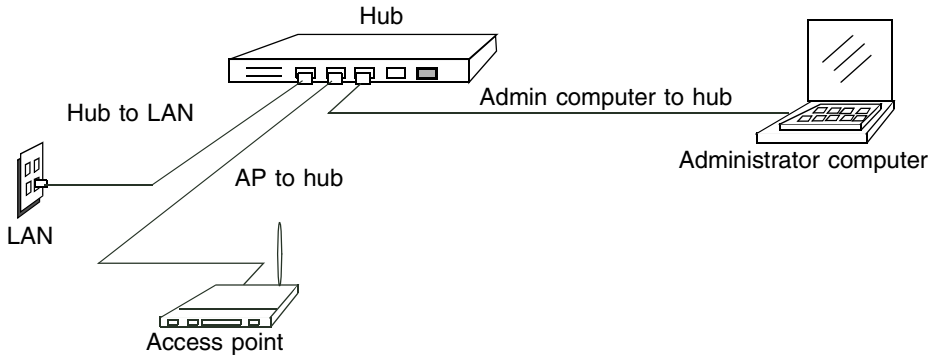
As new features and enhancements become available, you can upgrade the firmware to add new functionality and performance improvements to the access points that make up your wireless network. (See "Upgrading the firmware" on page 168.)

Connecting the access point to network and power

The next step is to set up the network and power connections.

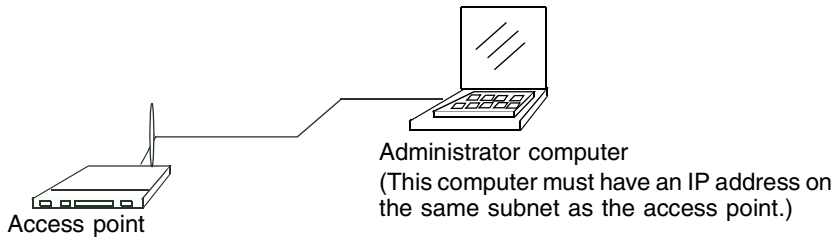
To set up the network and power connections:

1 Connect one end of an Ethernet cable to the network port on the access point and the other end to the same hub where your computer is connected.



OR -

Connect one end of an Ethernet cable to the network port on the access point and the other end of the cable to the Ethernet port on your computer.



Important

If you use a hub, the device you use must permit broadcast signals from the access point to reach all other devices on the network. A standard hub should work fine. Some switches, however, do not allow directed or subnet broadcasts through. You may have to configure the switch to allow directed broadcasts.

If for initial configuration use a direct wired connection (using an Ethernet cable) between the access point and your computer, you will need to reconfigure the cabling for subsequent startup and deployment of the access point so that the access point is no longer connected directly to your computer but instead is connected to the LAN (either using a Hub or directly).

It is possible to detect access points on the network (using Kickstart) with a wireless connection. However, we strongly advise against using this method. In most environments you may have no way of knowing whether you are actually connecting to the intended AP and also because many of the initial configuration changes required will cause you to lose connectivity with the AP over a wireless connection.

2 Connect the power adapter to the power port on the back of the access point, then plug the other end of the power cord into a power outlet (preferably, using a surge protector).

Setting up connections for a guest network

The Gateway 7001 Series self-managed AP offers an out-of-the-box Guest Interface that lets you configure an access point for controlled guest access to the network. The same access point can function as a bridge for two different wireless networks: A secure *Internal LAN* and a public *Guest* network. This can be done in one of two ways:

- Physically, by connecting the two LAN ports on the access point to different networks with two different cables, one to the internal LAN and the other to the public Guest network.
- Virtually, by defining two different Virtual LANs through the Administration UI.

Hardware connections for a guest VLAN

If you plan to configure a guest network using VLANs, do the following:

- Connect eth0 to a VLAN-capable switch
- Define VLANs on that switch

Hardware connections for a physically separate guest network

If you plan to configure a physically separate guest network, you need to set up your network connections differently at this point. The Gateway 7001 Series self-managed AP ships with an extra network port to support configuration of a physically separate guest network. Use both network ports on the access point to create two physical connections to different networks:

- Create a wired (Ethernet) connection from one of the network ports on the access point to your internal LAN.
- Create a second wired (Ethernet) connection from the other network port on the access point to a separate network.

After you have the required physical connections set up, the rest of the configuration process is accomplished through the Administration UI. For information on configuring guest interface settings on the Administration UI, see "Advanced Configuration" on page 67.

Turning on the access point

Plug in the AC power adapter and plug the power adapter into the Gateway 7001 Series self-managed AP, then wait for its initialization process to complete.

Running KickStart to find access points and assign IP addresses

KickStart is an easy-to-use utility for discovering and identifying new Gateway access points. KickStart scans the network looking for Gateway access points, and displays ID details on those it finds.

Important

Keep in mind that KickStart (and the other Gateway administration tools) recognizes and configures only Gateway 7001 Series self-managed APs. KickStart will not find or configure other kinds of access points or other devices.

Run Kickstart only in the subnet of the “Internal” network (SSID). Do not run Kickstart on the guest subnetwork.

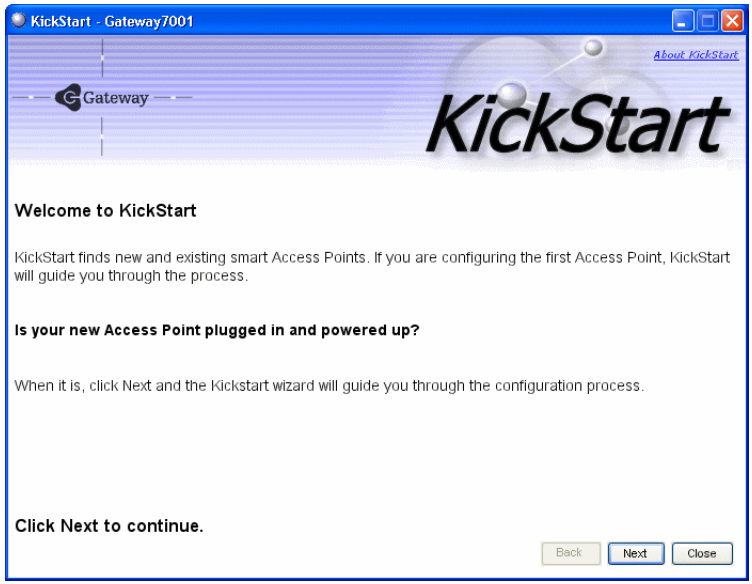
Kickstart will find only those access points that have IP addresses. IP addresses are dynamically assigned to APs if you have a DHCP server running on the network. Keep in mind that if you deploy the AP on a network with no DHCP server, the default static IP address (192.168.1.1) will be used.

Use caution with non-DHCP enabled networks: Do not deploy more than one new AP on a non-DHCP network unless you change the IP address list in the first DHCP server, because they will use the same default static IP addresses and conflict with each other. (For more information, see “Understanding dynamic and static IP addressing” on page 12 and “How does the access point obtain an IP address at startup?” on page 12.)

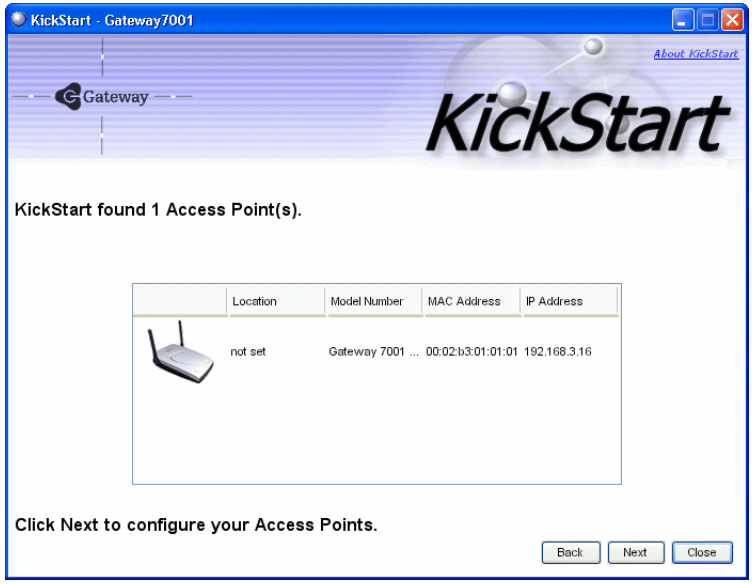
Run the KickStart CD on a laptop or computer that is connected to the same network as your access points and use it to step through the discovery process.

To run KickStart:

1 Insert the KickStart Wizard CD into the CD drive on your computer. If the KickStart window is not displayed automatically, navigate to the CD drive and double-click the Kickstart executable file to activate the KickStart utility on the CD. The *KickStart Welcome* screen is displayed.



2 Click **Next** to search for access points. Wait for the search to complete, or until KickStart has found your new access points.



Important

If no access points are found, Kickstart indicates this and presents some troubleshooting information about your LAN and power connections. After you have checked hardware power and Ethernet connections, you can click the Kickstart **Back** button to search again for access points.

3 Review the list of access points found.

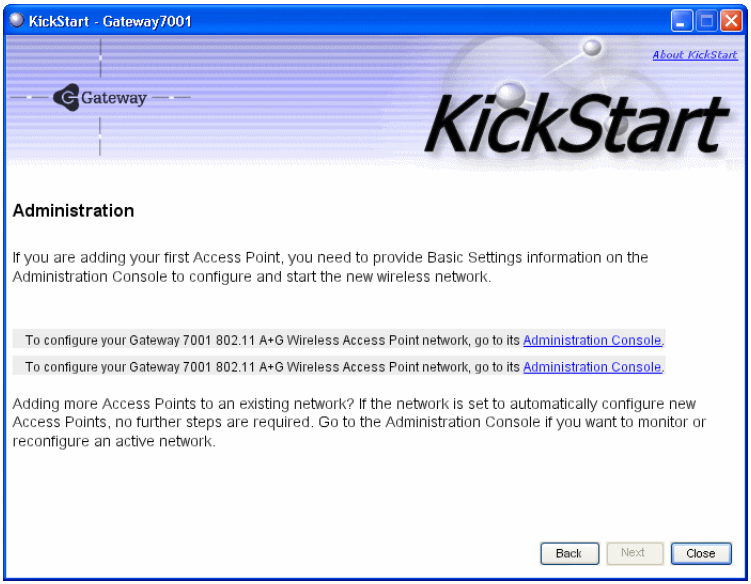
KickStart will detect the IP addresses of Gateway 7001 Series self-managed APs. Access points are listed with their locations, Media Access Control (MAC) addresses, and IP Addresses. If you are installing the first access point on a single-access-point network, only one entry will be displayed on this screen.

Verify the MAC addresses shown here against the hardware labels for each access point. This will be especially helpful later in providing or modifying the descriptive location name for each access point. Click **Next** to continue.

4 Go to the Access Point Administration Web pages by clicking the link provided on the KickStart page (see "Logging on to the administration Web pages" on page 24).

Important

KickStart provides a link to the Administration Web pages through the IP address of the first access point. The Administration Web pages are a centralized management tool that you can access through the IP address for any access point in a cluster. After your other access points are configured, you can also link to the Administration Web pages by using the IP address for any of the other Gateway access points in a URL (http://IPAddressOfAccessPoint).



Logging on to the administration Web pages

When you follow the link from KickStart to the Gateway 7001 Series self-managed AP administration Web pages, you are prompted for a user name and password.

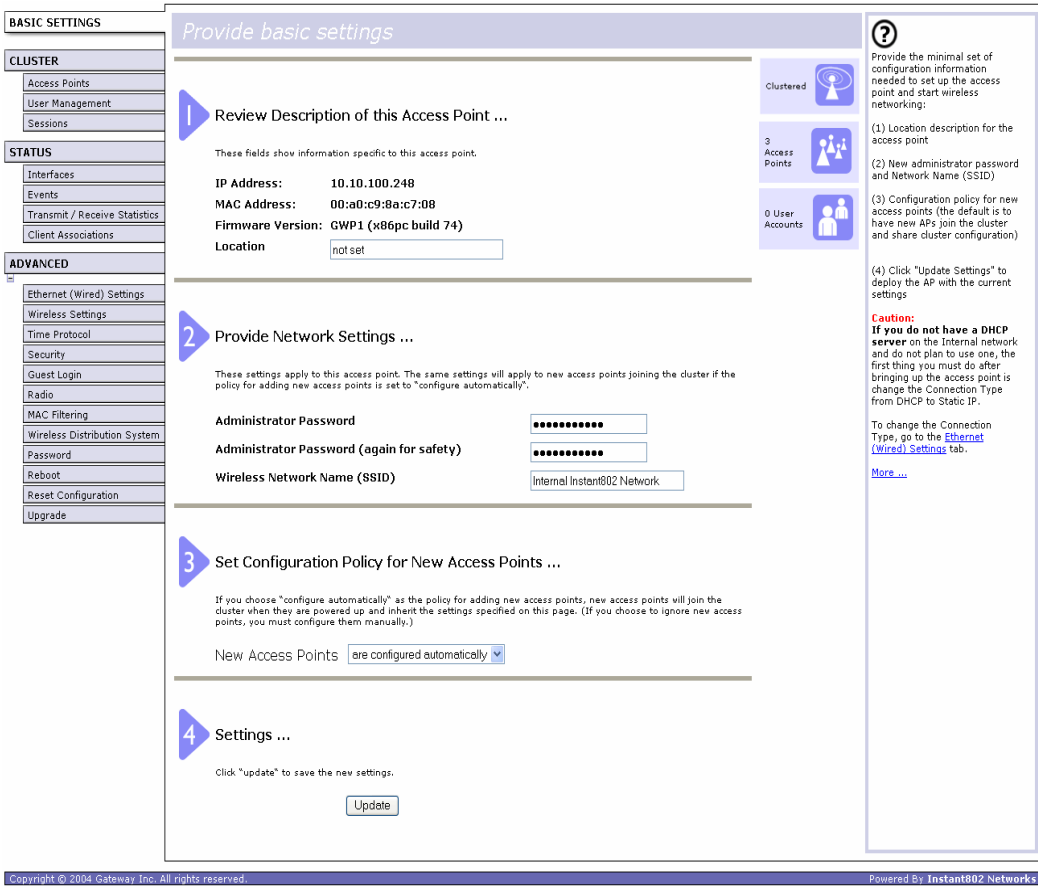
The defaults for user name and password are as follows.

Field	Default Setting
User name	admin
Password	admin The user name is read-only. It cannot be modified.

Type the user name and password and click **OK**.

Viewing basic settings for Gateway 7001 Series self-managed access points

When you log in, the *Basic Settings* page for Gateway 7001 Series self-managed AP administration is displayed. These are global settings for all access points that are members of the cluster and, if automatic configuration is specified, for any new access points that are added later.



Configuring basic settings and starting the wireless network

Provide a minimal set of configuration information by defining the basic settings for your wireless network. These settings are all available on the *Basic Settings* page of the Administration Web interface, and are categorized into steps 1-4 on the Web page.

To configure the basic settings:

1. Review the description of this access point and provide IP addressing information. For more information, see "Reviewing and describing the access point" on page 31.
2. Provide a new administrator password for clustered access points. For more information, see "Providing administrator password and wireless network name" on page 32.
3. Set configuration policy for new access points.

   Choose to configure new access points automatically (as new members of the cluster) or ignore new access points.

   If you set a configuration policy to configure new access points automatically, new access points added to this network will join the cluster and be configured automatically based on the settings you defined here. Updates to the network settings on any cluster member will be shared with all other access points in the group.

   If you chose to ignore new access points, then as you add new access points they will run in standalone mode. In standalone mode, an access point does not share the cluster configuration with other access points. Instead it must be configured manually.

   You can always update the settings on a standalone access point to have it join the cluster. You can also remove an access point from a cluster thereby switching it to run in standalone mode.

   For more information, see "Setting configuration policy for new access points" on page 34.
4. Start wireless networking by clicking **Update** to activate the wireless network with these new settings. For more information, see "Updating basic settings" on page 36.

Default configuration

If you follow the steps above and accept all the defaults, the access point will have the default configuration described in "Default settings and supported administrator/client platforms" on page 5.

What's next?

Make sure the access point is connected to the LAN and access some wireless clients. After you have tested the basics of your wireless network, you can enable more security and fine-tune by modifying advanced configuration features.

Make sure the access point is connected to the LAN

If you configured the access point and administrator computer by connecting both into a network hub, then your access point is already connected to the LAN. The next step is to test some wireless clients.

To test wireless clients:

1. If you configured the access point using a direct wired connection with an Ethernet cable from your computer to the access point, disconnect the cable from your computer and the access point.
2. Connect a regular Ethernet cable from the access point to the LAN.
3. Connect your computer to the LAN either through Ethernet cable or wireless client card.

Test LAN connectivity with wireless clients

Test the Gateway 7001 Series self-managed AP by trying to detect it and associate with it from some wireless client devices. (See "Wireless client computers" on page 11 in the PreLaunch Checklist: Default Settings and Supported Administrator/Client Platforms for information on requirements for these clients.)

Secure and fine-tune the access point using advanced features

After you have the wireless network up and running and have tested against the access point with some wireless clients, you can add in more layers of security, add users, configure a guest interface, and fine-tune performance settings.

Chapter 3

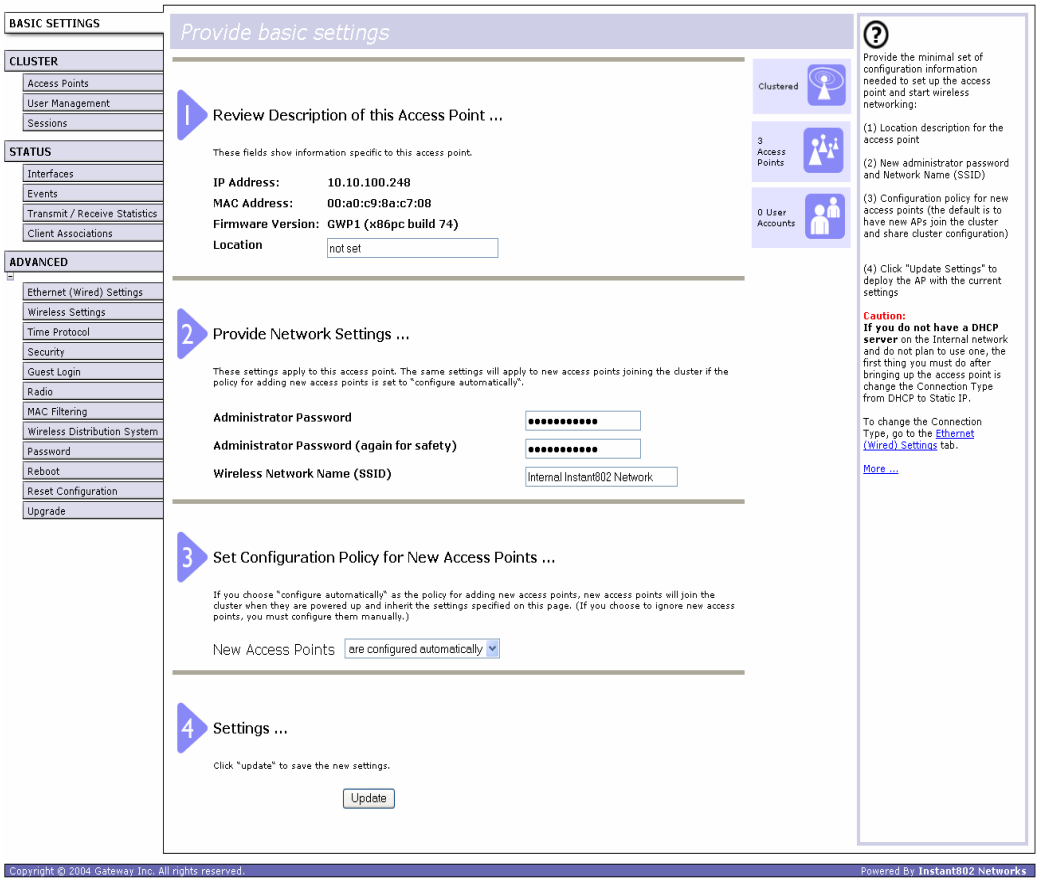
Configuring Basic Network Settings

- Navigating to basic settings
- Reviewing and describing the access point
- Setting configuration policy for new access points
- Understanding basic settings for a standalone access point
- Understanding indicator icons

Navigating to basic settings

To configure basic Network settings, click **Network**, then click **Basic Settings**.

If you use Kickstart to link to the Administration Web pages, the *Basic Settings* page is displayed by default.

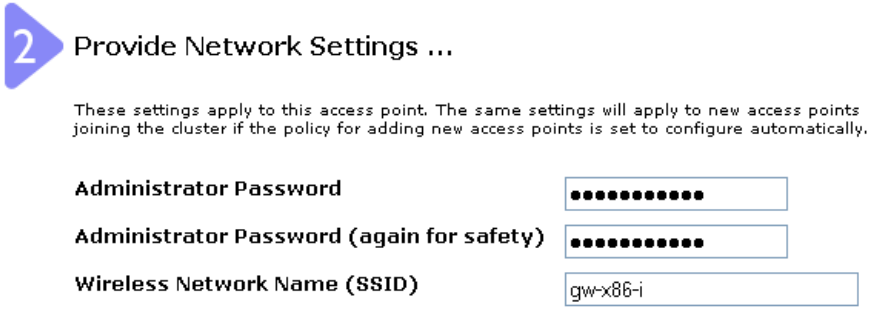


Fill in the boxes on the *Basic Settings* page as described in the following section.

Reviewing and describing the access point

Field	Action
IP Address	This box is not editable because the IP address is already assigned (either through DHCP, or statically through the Ethernet (Wired) settings as described in "Configuring Guest interface Ethernet settings" on page 73).
MAC Address	A MAC address is a permanent, unique hardware address for any device that represents an interface to the network. The MAC address is assigned by the manufacturer. You cannot change the MAC address. It is provided here for informational purposes as a unique identifier for an interface. The address shown here is the MAC address for the bridge (br0). This is the address by which the AP is known externally to other networks. To see MAC addresses for guest and internal interfaces on the AP, see the **Status > Interfaces** tab.
Firmware Version	Version information about the firmware currently installed on the access point. As new versions of the Gateway 7001 Series self-managed AP firmware become available, you can upgrade the firmware on your access points to take advantages of new features and enhancements. For instructions on how to upgrade the firmware, see "Upgrading the firmware" on page 168.
Location	Specify a location description for this access point.

Providing administrator password and wireless network name



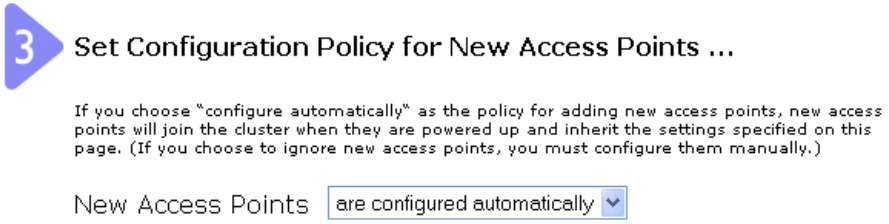
Caution

The Gateway 7001 Series self-managed AP is not designed for multiple, simultaneous configuration changes. If you have a network that includes multiple access points, and more than one administrator is logged on to the Administration Web pages and making changes to the configuration, all access points in the cluster will stay in synch but there is no guarantee that all configuration changes specified by multiple users will be applied.

Field	Action
Administrator Password	Type a new administrator password. The characters you enter will be displayed as "*" characters to prevent others from seeing your password as you type. The Administrator password must be an alphanumeric strings of up to 32 characters. Do not use special characters. **Note:** As an immediate first step in securing your wireless network, we recommend that you change the administrator password from the default.
Administrator Password (again)	Re-type the new administrator password to confirm that you typed it as intended.

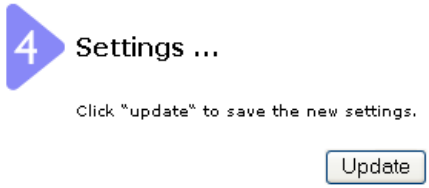
Field	Action
Wireless Network Name (SSID)	Type a name for the wireless network as a character string. This name will apply to all access points on this network. As you add more access points, they will share this SSID. The *Service Set Identifier* (SSID) is an alphanumeric string of up to 32 characters **Note:** If you are connected as a wireless client to the same AP that you are administering, resetting the SSID will cause you to lose connectivity to the AP. You will need to reconnect to the new SSID after you save this new setting.

Setting configuration policy for new access points



Field	Action
New Access Points	Choose the policy you want to put in effect for adding New Access Points to the network. • If you choose **are configured automatically**, then when a new access points is added to the network it automatically joins the existing *cluster*. The cluster configuration is copied to the new access point, and no manual configuration is required to deploy it. • If you choose **are ignored**, new access points will not join the cluster, but will be considered *standalone*. You need to configure standalone access points manually through KickStart and the Administration Web pages residing on the standalone access points. (To get to the Web page for a standalone access point, use its IP address in a URL as follows: http://*IPAddressOfAccessPoint*.). **Note:** If you change the policy so that new access points are ignored, then any new access points you add to the network will not join the cluster. Existing clustered access points will not be aware of these standalone APs. Therefore, if you are viewing the Administration Web pages through the IP address of a clustered access point, the new standalone APs will not show up in the list of access points on the **Cluster > Access Points** tab. The only way to see a standalone AP is to browse to it directly by using its IP address in the URL. If you later change the policy back to the default so that new access points "are configured automatically," all subsequent new APs will automatically join the cluster. Standalone APs, however, will stay in standalone mode until you explicitly add them to the cluster. For information on how to add standalone APs to the cluster, see "Adding an access point to a cluster" on page 52.

Updating basic settings



When you have reviewed the new configuration, click **Update** to apply the settings and deploy the access points as a wireless network.

Understanding basic settings for a standalone access point

The **Basic Settings** tab for a standalone access point indicates only that the current mode is standalone and provides a button for adding the access point to a cluster (group). If you click on any of the **Cluster** tabs on the Administration pages for an access point in standalone mode, you will be re-directed to the Basic Settings page because Cluster settings do not apply to standalone APs.

For more information, see "Standalone mode" on page 44 and "Adding an access point to a cluster" on page 52.

Understanding indicator icons

All the network settings tabs on the Administration Web pages include visual indicator icons showing current network activity

Icon	Description
	The clustering icon indicates whether the current access point is “Clustered” or “Not Clustered” (that is, standalone).
	The number of access points available for service on this network is indicated by the “Access Points” icon.
	Then number of client user accounts created and enabled on this network is indicated by the “User Accounts” icon.

Chapter 4

Managing Access Points and Clusters

- Navigating to access points management
- Understanding clustering and access points
- Modifying the location description
- Adding and removing an access point
- Navigating to an AP by using its IP address in a URL

Introduction

The Gateway 7001 Series self-managed APs show current basic configuration settings for clustered access points (location, IP address, MAC address, status, and availability) and provide a way of navigating to the full configuration for specific APs if they are cluster members.

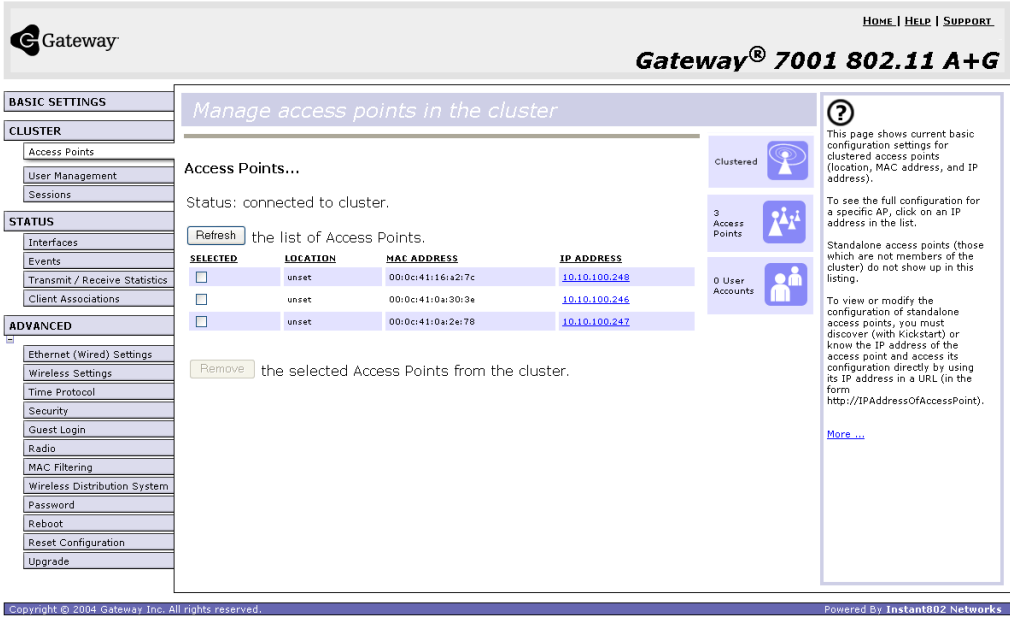
Standalone access points (those which are not members of the cluster) do not show up in this listing. To configure standalone access points, you must discover (through Kickstart) or know the IP address of the access point and by using its IP address in a URL (http://IPAddressOfAccessPoint).

Important

The Gateway 7001 Series self-managed APs are not designed for multiple, simultaneous configuration changes. If you have a network that includes multiple access points, and more than one administrator is logged on to the Administration Web pages and making changes to the configuration, all access points in the cluster will stay in synch but there is no guarantee that all configuration changes specified by multiple users will be applied.

Navigating to access points management

To view or edit information on access points in a cluster, click **Cluster > Access Points** on the Administration Web page. The *Manage access points in the cluster* screen opens.



Understanding clustering

A key feature of the Gateway 7001 Series self-managed AP is the ability to form a dynamic, configuration-aware group (called a cluster) with other Gateway access points in a network in the same subnet.

Access points can participate in a peer-to-peer cluster which makes it easier for you to deploy, administer, and secure your wireless network. The cluster provides a single point of administration and lets you view the deployment of access points as a single wireless network rather than a series of separate wireless devices.

What is a cluster?

A cluster is a group of access points which are coordinated as a single group through Gateway 7001 Series self-managed AP administration. You cannot create multiple clusters on a single wireless network (SSID).

Only one cluster per wireless network is supported.

How many APs can a cluster support?

The Gateway 7001 Series self-managed AP can support up to eight access points in a cluster at any one time. If a new AP is added to a network with a cluster that is already at full capacity, the new AP is added in *stand-alone mode*. Note that when the cluster is full, extra APs are added in stand-alone mode regardless of the configuration policy in effect for new access points.

For related information, see "Cluster mode" on page 44, "Standalone mode" on page 44, and "Setting configuration policy for new access points" on page 34.

What kinds of APs can cluster together?

A Gateway 7001 Series self-managed AP can form a cluster with itself (a "cluster of one") and with other Gateway 7001 Series self-managed APs that share some basic characteristics. In order to be members of the same cluster, access points must be Gateway 7001 Series self-managed APs:

- Of the same radio configuration (all dual-band APs or all single-band APs)
- On the same LAN

A dual-band and a single-band AP cannot be members of the same cluster. Therefore, a Gateway 7001 802.11 A+G Wireless Access Point (dual-band) cannot cluster with a Gateway 7001 802.11 G Wireless Access Point (single-band). Also, Gateway 7001 Series self-managed APs will not cluster with non Gateway APs.

Having a mix of APs on the network does not adversely affect Gateway 7001 Series self-managed AP clustering in any way, however it is helpful to understand the clustering behavior for administration purposes:

- Gateway 7001 Series self-managed APs of the same model will form a cluster. The dual-band APs will form one cluster and the single-band APs will form another cluster.
- Non-Gateway APs will not join Gateway clusters. They should be administered as usual through their associated Administration tools.

Which settings are shared in the cluster configuration and which are not?

Most configuration settings defined through the Gateway 7001 Series self-managed AP Administration Web pages will be propagated to cluster members as a part of the cluster configuration.

Settings shared in the cluster configuration

The cluster configuration includes:

- Network name (SSID)
- Administrator password
- Configuration policy
- User accounts and authentication
- Wireless interface settings
- Radio settings
- QoS queue parameters
- MAC address filtering.

Settings not shared by the cluster

The few exceptions (settings not shared among clustered access points) are the following most of which, by nature, must be unique:

- IP addresses
- MAC addresses
- Location descriptions
- WDS bridges
- Security settings
- Ethernet (Wired) Settings, including enabling or disabling Guest access
- Guest interface configuration

Settings that are not shared must be configured individually on the Administration pages for each access point. To get to the Administration pages for an access point that is a member of the current cluster, click on its IP Address link on the *Cluster > Access Points* page of the current AP.

Cluster mode

When an access point is a cluster member, it is considered to be in cluster mode. You define whether you want new access points to join the cluster or not through the configuration policy you set in Basic Settings. (See "Setting configuration policy for new access points" on page 34.) You can re-set an access point in cluster mode to standalone mode. (See "Removing an access point from the cluster" on page 51.)

Important

When the cluster is full (eight APs is the limit), extra APs are added in *stand-alone mode* regardless of the configuration policy in effect for new access points. See "How many APs can a cluster support?" on page 42.

Gateway 7001 Series self-managed APs of different models form separate clusters. See "What kinds of APs can cluster together?" on page 42.

Standalone mode

Gateway 7001 Series self-managed APs can be configured in standalone mode. In standalone mode, an access point is not a member of the cluster and does not share the cluster configuration, but rather requires manual configuration that is not shared with other access points. (See "Setting configuration policy for new access points" on page 34 and "Removing an access point from the cluster" on page 51.)

Standalone access points are not listed on the **Cluster > Access Points** tab in the Administration UI.

You need to know the IP address for a standalone access point in order to configure and manage it directly. (See "Navigating to an AP by using its IP address in a URL" on page 53.)

The Basic Settings tab for a standalone access point indicates only that the current mode is standalone and provides a button for adding the access point to a cluster (group). If you click on any of the Cluster tabs on the Administration pages for an access point in standalone mode, you will be redirected to the Basic Settings page because Cluster settings do not apply to stand-alone APs.

Important

When the cluster is full (eight APs is the limit), extra APs are added in *stand-alone mode* regardless of the configuration policy in effect for new access points. See "How many APs can a cluster support?" on page 42.

You can re-enable cluster mode on a standalone access point. (See “Adding an access point to a cluster” on page 52.)

Cluster formation

A cluster is formed when the first Gateway 7001 Series self-managed AP is configured. (See “Quick Setup” on page 15 and “Configuring Basic Network Settings” on page 29.)

If a cluster configuration policy is in place when a new access point is deployed, it attempts to rendezvous with an existing cluster.

If it is unable to locate a cluster, then it establishes a new cluster on its own.

If it locates a cluster but is rejected because the cluster is full, or the clustering policy is to ignore new access points, then the access point will deploy in standalone mode.

Cluster size and membership

The upper limit of a cluster is eight access points. The Network Web administration page provides a real-time, visual indicator of the number of access points in the current cluster and warns when the cluster has reached capacity. (See “Configuring basic settings and starting the wireless network” on page 27.)

If a cluster is present but is already full, new access points will deploy in standalone mode.

Intra-cluster security

To make sure that the security of the cluster as a whole is equivalent to the security of a single access point, communication of certain data between access points in a cluster is done using *Secure Sockets Layer* (typically referred to as SSL) with private key encryption.

Both the cluster configuration file and the user database are transmitted among access points using SSL.

Auto-Synch of Cluster Configuration

If you are making changes to the AP configuration that require a relatively large amount of processing (such as adding several new users), you may encounter a synchronization progress bar after clicking **Update** on any of the Administration pages. The progress bar indicates that the system is busy performing an auto-synch of the updated configuration to all APs in the cluster. The Administration Web pages are not editable during the auto-synch.

Note that auto-synchronization always occurs during configuration updates that affect the cluster, but the processing time is usually negligible. The auto-synch progress bar is displayed only for longer-than-usual wait times.

Cluster recovery

In cases where the access points in a cluster become out of sync for any of the reasons mentioned in "Known problems" on page 172, or an access point cannot join or be removed from a cluster, the following methods for cluster recovery are recommended.

Reboot or reset access point

These recovery methods are given in the order you should try them. In all but the last case (stop clustering), you only need to reset or reboot the particular access point whose configuration is out of sync with other cluster members or cannot remove/join cluster.

- Reboot the access point from its Administration UI. To do this, go to http://*IPAddressOfAccessPoint*, navigate to **Advanced > Reboot** and click **Reboot**. (IP addresses for APs are on the *Cluster > Access Points* page for cluster members.)
- Physically reboot the access point by pressing the Power button on the device.
- Reset the access point from its Administration UI. To do this, go to http://*IPAddressOfAccessPoint*, navigate to **Advanced > Reset Configuration**, and click **Reset**. (IP addresses for APs are on the *Cluster > Access Points* page for any cluster member.)
- Physically reset the access point by pressing the Reset button on the device.
- In some extreme cases, reboot or reset may not solve the problem. In these cases, follow the procedure described the next section.

Stop clustering and reset each access point in the cluster

If the previous reboot or reset methods do not solve the problem, do the following to stop clustering and reset all APs.

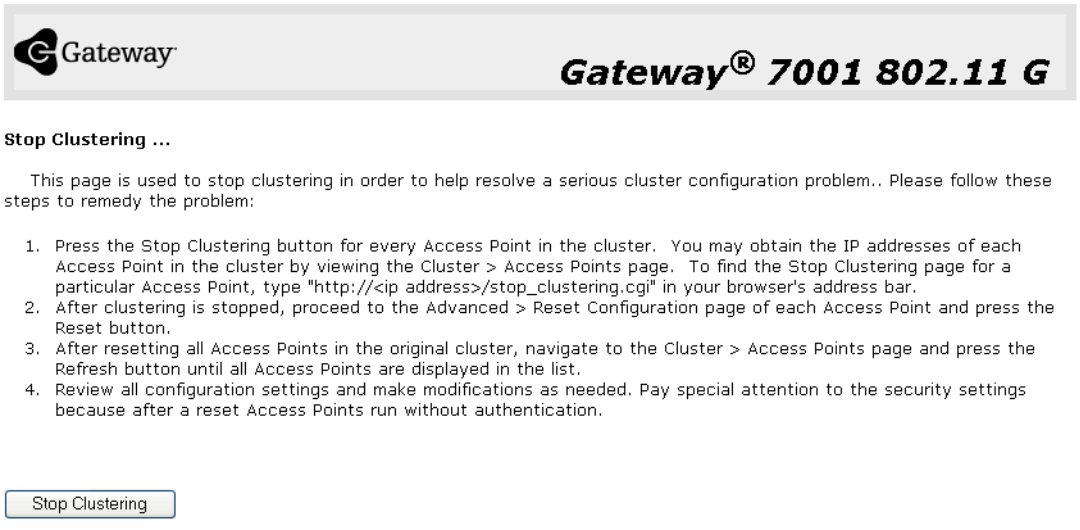
To stop clustering and reset each access point in the cluster:

1. Stop clustering on each access point in the cluster by entering the Stop Clustering URL in the address bar of your Web browser as follows:

   http://*IPAddressOfAccessPoint*/stop_clustering.cgi

   Where *IPAddres0sOfAccessPoint* is the IP address of the access point you want to stop clustering. You can find the IP addresses for the cluster members on the *Cluster > Access Points* page for any of the clustered access points. We recommend making a note of all IP addresses at this point.

The *Stop Clustering* page for this access point opens.



2 Click the **Stop Clustering** button.

3 Repeat steps 1 and 2 for every access point in the cluster.

Caution

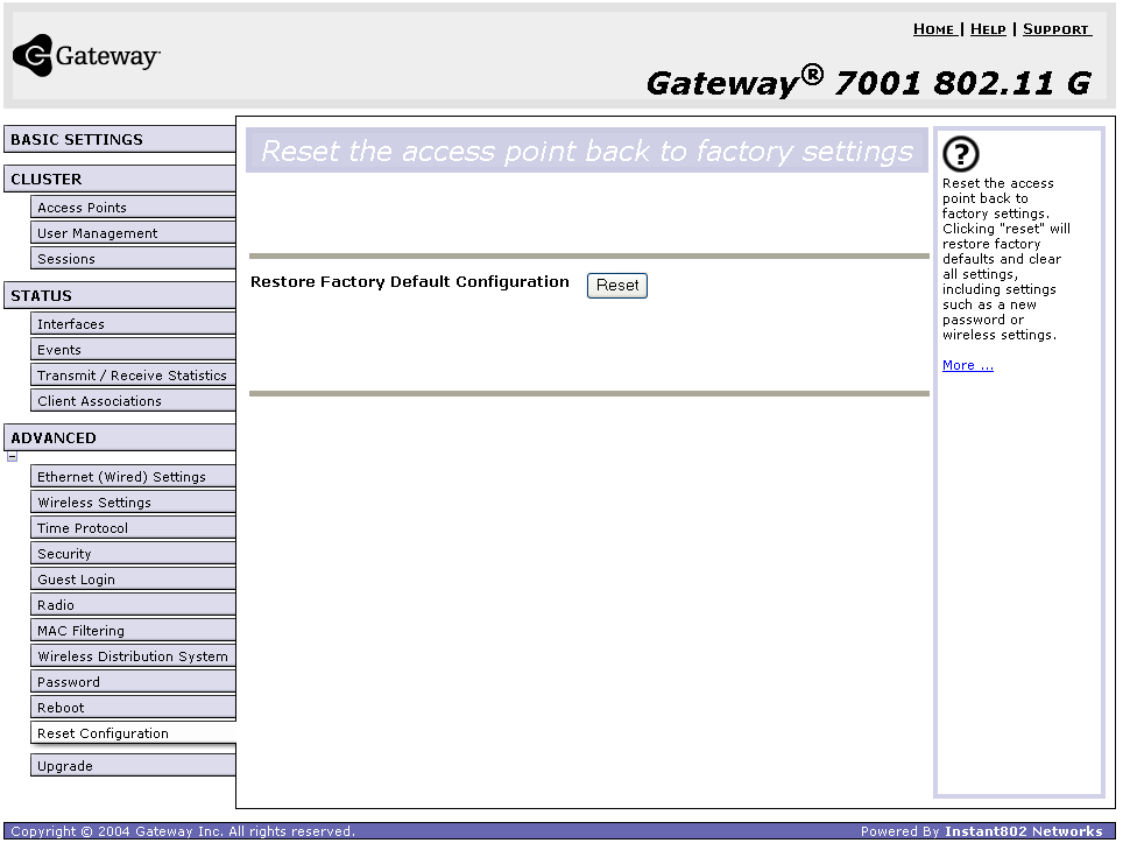
Do not proceed to the next step of resetting any access points until you have stopped clustering on all of them. Make sure that you first "Stop Clustering" on every access point on the subnet, and only then perform the next part of the process of resetting each one to the factory defaults.

4 Reset each access point by going to the Administration Web pages of the access point you want to reset by entering its URL into the address bar of your Web browser:

http://*IPAddressOfAccessPoint*/

Where *IPAddres0sOfAccessPoint* is the IP address of the access point you want to reset.

5 On the Administration UI left-hand tabs, click **Advanced > Reset Configuration** to open the *Reset* page. The *Reset* page opens.



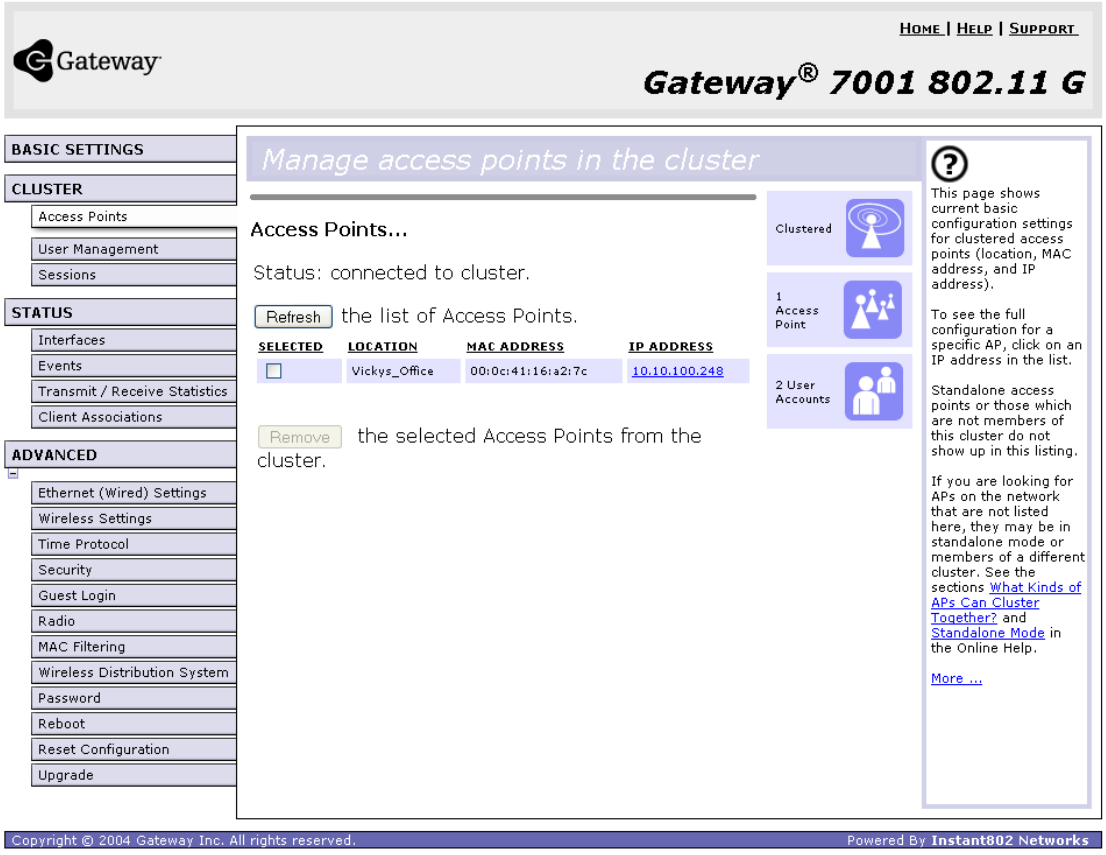
6 Click **Reset** to restore the factory defaults on the access point. (This will clear all of your previous settings, including updated passwords.)

7 Repeat steps 4 through 6 for every access point in the cluster.

Caution

Do not proceed to the next step until you have stopped clustering on all of access points in the pre-existing cluster.

8 Refresh the cluster view by clicking **Cluster > Access Points** on the Administration Web pages for any one of the access points. The *Access Points cluster management* page opens.



9 Click **Refresh**.

At this point you should see all previous cluster members displayed in the list. Before proceeding to the last step, verify that the cluster has reformed by making sure all are access points are listed.

10 Review all configuration settings and make modifications as needed.

Pay special attention to the security settings because after a reset, access points run without any security in place.

Understanding access point settings

The **Access Points** tab on the Administration Web page provides information about all access points on the wireless network.

From this tab, you can view location descriptions, IP addresses, enable (activate) or disable (deactivate) clustered access points, and remove access points from the cluster. You can also modify the location description for an access point.

The IP address links provide a way to navigate to configuration settings and data on an access point.

Navigating to a specific access point can be particularly useful for access points running in standalone mode.

The following table describes the access point settings and information display in detail.

Field	Description
Location	Description of where the access point is physically located.
MAC Address	Media Access Control (MAC) address of the access point. A *MAC address* is a permanent, unique hardware address for any device that represents an interface to the network. The MAC address is assigned by the manufacturer. You cannot change the MAC address. It is provided here for informational purposes as a unique identifier for the access point. Even if an access point is configured for multiple BSSIDs and has multiple MAC addresses, only one of its MAC addresses will be shown in this list.
IP Address	Specifies the IP address for the access point. Each IP address is a link to the Administration Web pages for that access point. You can use the links to navigate to the Administration Web pages for a specific access point. This is useful for viewing data on a specific access point to make sure a cluster member is picking up cluster configuration changes, to configure advanced settings on a particular access point, or to switch a standalone access point to cluster mode.

Working with access points in a cluster

Modifying the location description

To make modifications to the location description:

1. Click **Basic Settings** on the Administration Web page.
2. Update the location description in section 1 under "Review Description of this Access Point."
3. Click **Update** to apply the changes.

Removing an access point from the cluster

To remove an access point from the cluster:

1. Click **Cluster > Access Points** on the Administration Web page. The *Manage access points in the cluster* screen opens.
2. Click the box next to the access point you want to disable.
3. Click **Remove from Cluster.**

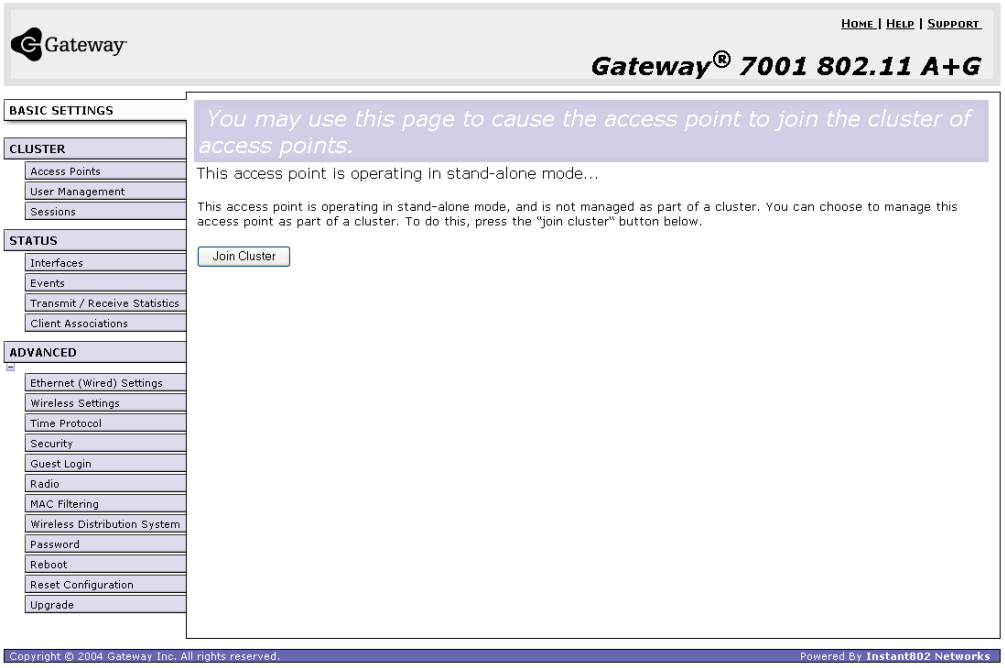
   The change will be reflected under Status for that access point and it will now show as standalone (instead of cluster).

Adding an access point to a cluster

To add an access point that is currently in standalone mode back into a cluster:

1 Go to the Administration Web pages for the standalone access point. (See "Navigating to an AP by using its IP address in a URL" on page 53.)

The Administration Web page for the standalone access point is displayed.



2 Click the **Basic Settings** tab in the Administration pages for the standalone access point.

The **Basic Settings** tab for a standalone access point indicates that the current mode is standalone and provides a button for adding the access point to a cluster (group).

Important

When the cluster is full (eight APs is the limit), extra APs are added in *stand-alone mode* regardless of the configuration policy in effect for new access points. See "How many APs can a cluster support?" on page 42.

3 Click **Join Cluster**. The access point is now a cluster member. Its Status (Mode) on the **Cluster > Access Points** tab now indicates **cluster** instead of **standalone**.

Navigating to information for a specific AP and managing standalone APs

In general, Gateway 7001 Series self-managed APs are designed for central management of clustered access points. For access points in a cluster, all access points in the cluster reflect the same configuration. In this case, it does not matter which access point you actually connect to for administration.

There may be situations, however, when you want to view or manage information on a particular access point. For example, you might want to check status information such as client associations or events for an access point. Or you might want to configure and manage features on an access point that is running in standalone mode. In these cases, you can navigate to the Administration Web interface for individual access points by clicking the IP address links on the Access Points tab.

All clustered access points are shown on the *Cluster* > *Access Points* page. To navigate to clustered access points, you click on the IP address for a specific cluster member shown in the list.

Navigating to an AP by using its IP address in a URL

You can also link to the Administration Web pages of a specific access point, by typing the IP address for that access point as a URL directly into a Web browser address bar in the following form:

http://IPAddressOfAccessPoint

(where IPAddressOfAccessPoint is the address of the particular access point you want to monitor or configure).

For standalone access points, this is the only way to navigate to their configuration information. If you do not know the IP address for a standalone access point, use Kickstart to find all APs on the network and you should be able to derive which ones are standalone by comparing KickStart findings with access points listed on the **Cluster > Access Points** tab. The APs that Kickstart finds that are not shown on the this tab are probably standalone APs. (For more information on using Kickstart, see "Running KickStart to find access points and assign IP addresses" on page 20.)

Chapter 5

Managing User Accounts

- Navigating to user management for clustered access points
- Viewing and changing user accounts
- Adding a user
- Editing a user accountt
- Enabling and disabling user accounts
- Removing a user

Introduction

The Gateway 7001 Series self-managed APs include user management capabilities for controlling client access to access points.

User management and authentication must always be used in conjunction with the following two security modes, which require use of a RADIUS server for user authentication and management.

- IEEE 802.1x mode (see "IEEE 802.1x" on page 93 in Configuring network security)
- WPA with RADIUS mode (see "WPA with RADIUS" on page 95 in Configuring network security)

You have the option of using either the internal RADIUS server embedded in the Gateway 7001 Series self-managed AP or an external RADIUS server that you provide. If you use the Gateway 7001 Series self-managed AP embedded RADIUS server, use this Administration Web page on the access point to set up and manage user accounts. If you are using an external RADIUS server, you need to set up and manage user accounts on the Administrative interface for that server.

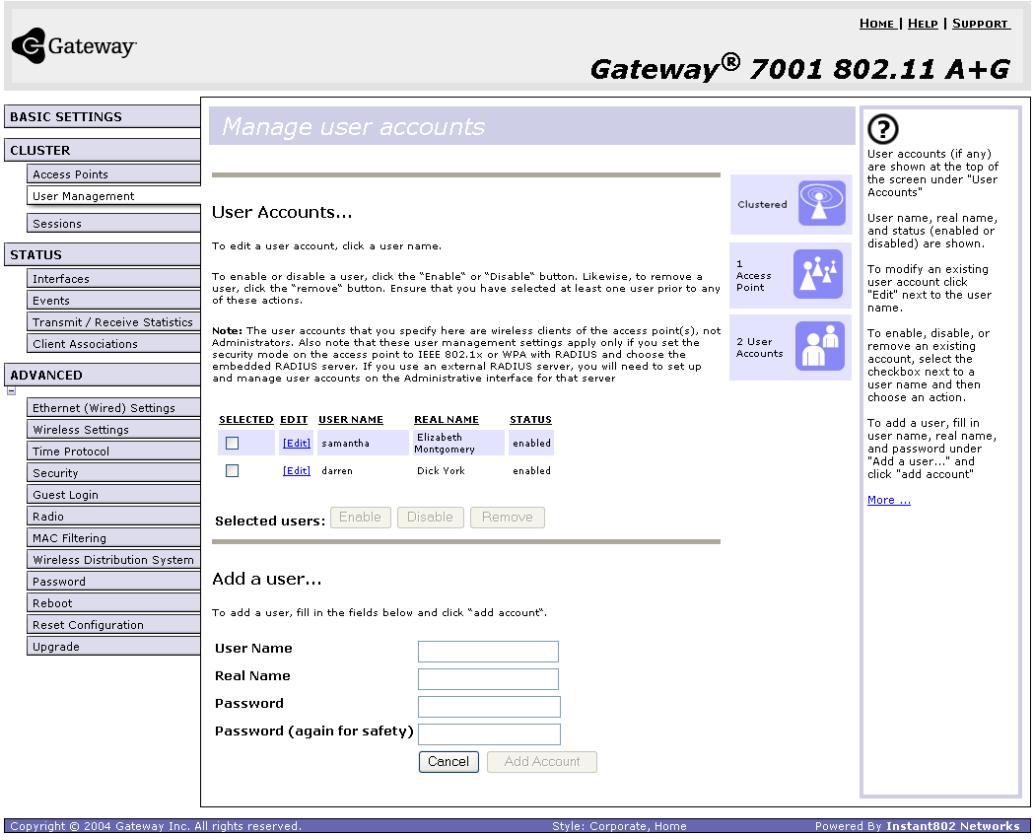
On the User Management page, you can create, edit, remove, and view client *user accounts*. Each user account consists of a user name and password. The set of users specified here represent approved *clients* that can log in and use one or more access points to access local and possibly external networks via your wireless network.

Important

Users specified here are clients of the Gateway access point(s) who use the APs as a connectivity hub, not administrators of the wireless network. Only those with the administrator user name and password and knowledge of the administration URL can log in as an administrator and view or modify configuration settings.

Navigating to user management for clustered access points

To set up or modify user accounts, click **Cluster > User Management** on the *Administration* Web page. The *Manage user accounts* screen opens.



Viewing and changing user accounts

Viewing user accounts

User accounts are shown at the top of the *Manage user accounts* screen under User Accounts. User name, real name and status (enabled or disabled) are shown. You can make modifications to an existing user account by first selecting the checkbox next to a user name then choosing an action. (See "Editing a user account" on page 59)

Adding a user

To create a new user:

1 On the *Manage user accounts* screen, under **Add a User**, provide information in the following boxes.

Field	Description
User name	Provide a user name. User names are alphanumeric strings of up to 256 characters. Do not use special characters.
Real Name	For information purposes, provide the user's full name. There is a 256 character limit on real names.
Password	Specify a password for this user. Passwords are alphanumeric strings of up to 256 characters. Do not use special characters.

2 When you have filled in the boxes, click **Add Account** to add the account.

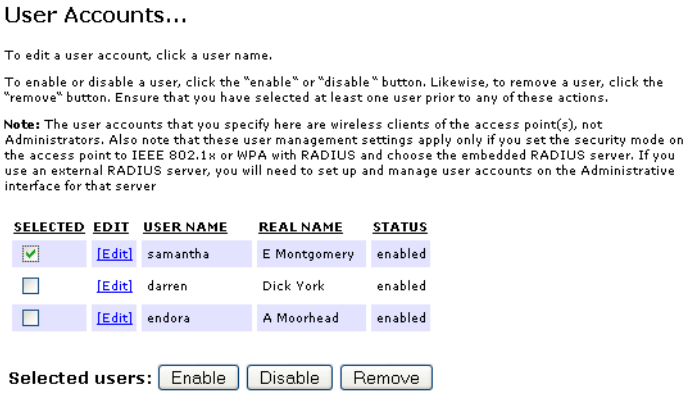
The new user is then displayed in User Accounts. The user account is enabled by default when you first create it.

Important

A limit of 100 user accounts per access point is imposed by the Administration user interface. Network usage may impose a more practical limit, depending on the demand from each user.

Editing a user account

After you have created a user account, it is displayed under User Accounts at the top of the *User Management* Web page. To make modifications to an existing user account, first click the checkbox next to the user name so that a checkmark is displayed in the box.



Then, choose an action such as **Edit**, **Enable**, **Disable**, or **Remove**.

Enabling and disabling user accounts

A user account must be enabled for the user to log on as a client and use the access point.

You can *enable* or *disable* any user account. With this feature, you can maintain a set of user accounts and authorize or prevent users from accessing the network without having to remove or re-create accounts. This is convenient in situations where users have an occasional need to access the network. For example, contractors who do work for your company on an intermittent but regular basis might need network access for 3 months at a time, then be off for 3 months, and back on for another assignment. You can enable and disable these user accounts as needed, and control access as appropriate.

To enable a user account:

- On the *User Management* Web page, under User Accounts, click the box next to the user name, then click **Enable**.

  A user with an account that is enabled can log on to the wireless access points in your network as a client.

To disable a user account:

- On the *User Management* Web page, under User Accounts, click the box next to the user name, then click **Disable**.

  A user with an account that is disabled cannot log on to the wireless access points in your network as a client. However, the user remains in the database and can be enabled later as needed.

To remove a user account:

- On the *User Management* Web page, under User Accounts, click the box next to the user name, then click **Remove**.

  If you think you might want to add this user back in at a later date, you might consider disabling the user rather than removing the account altogether.

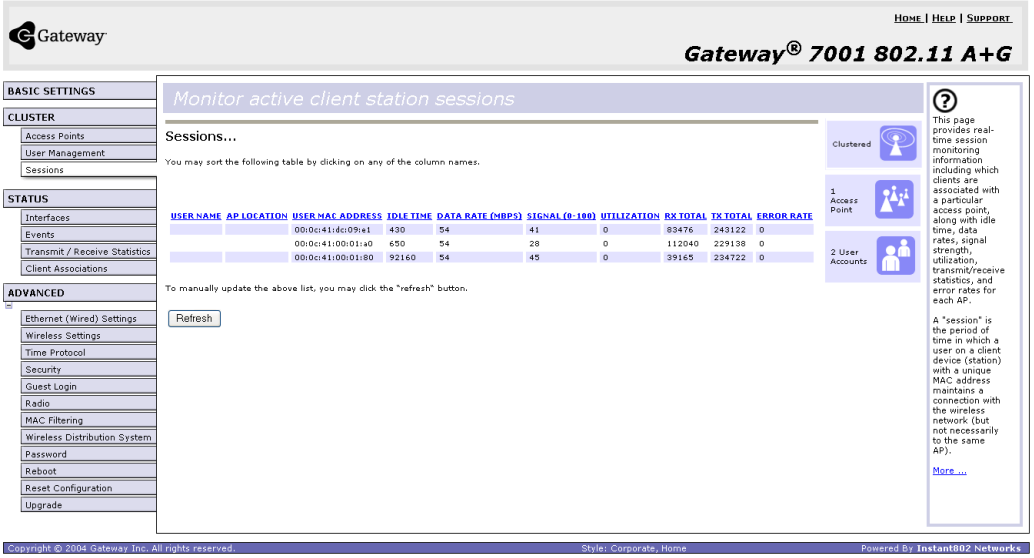
Chapter 6

Session Monitoring

- Navigating to session monitoring
- Understanding session monitoring information
- Viewing session information for access points
- Sorting session information
- Refreshing session information

Navigating to session monitoring

To view session monitoring information, click **Cluster > Sessions** on the Administration Web page. The *Monitor active client station sessions* page opens.



Understanding session monitoring information

The *Monitor active client station sessions* page shows the stations associated with access points in the cluster.

A *session* in this context is the period of time in which a user on a client device (station) with a unique MAC address maintains a connection with the wireless network. The session begins when the client logs on to the network, and the session ends when the client either logs off intentionally or loses the connection for some other reason.

Important

A session is not the same as an association, which describes a client connection to a particular access point. A client network connection can shift from one clustered AP to another within the context of the same session. A client station can roam between APs and maintain the session.

Details about the session information shown is described in the following table.

Field	Description
User Name	Indicates the client user name.
AP Location	Indicates the location of the access point. This is derived from the location description specified on the Basic Settings tab.
User MAC Address	Indicates the MAC address of the user's client device (station). A MAC address is a hardware address that uniquely identifies each node of a network.
Idle Time	Indicates the amount of time this station has remained inactive. A station is considered to be "idle" when it is not receiving or transmitting data.
Data Rate	The speed at which this access point is transferring data to the specified client. The data transmission rate is measured in megabits per second (Mbps). This value should fall within the range of the advertised rate set for the IEEE 802.1x mode in use on the access point. For example, 6 to 54Mbps for 802.11a.

Field	Description
Signal	Indicates the strength of the radio frequency (RF) signal the client receives from the access point. The measure used for this is an IEEE 802.1x value known as *Received Signal Strength Indication* (RSSI), and will be a value between 0 and 100. RSSI is determined by a an IEEE 802.1x mechanism implemented on the network interface card (NIC) of the client station.
Utilization	Utilization rate for this station. For example, if the station is “active” (transmitting and receiving data) 90% of the time and inactive 10% of the time, its “utilization rate” is 90%.
RxAve	Indicates number of total packets received by the client during the current session.
TxAve	Indicates number of total packets transmitted to the client during this session.
Error Rate	Indicates the percentage of time frames are dropped during transmission on this access point.

Viewing session information for access points

You can view session information for all access points on the network at the same time, or set the display to show session information for a specified access point chosen from the list at the top of the screen.

To view information on all access points, select the **Show all access points** option at the top of the page.

To view session information on a particular access point, select the **Show only this access point** option and choose the access point name from the list.

Sorting session information

To order (sort) the information shown in the tables by a particular indicator, click on the column label by which you want to order things. For example, if you want to see the table rows ordered by utilization rate, click **Utilization**. The entries will be sorted by utilization rate.

Refreshing session information

You can set the time in seconds for this screen to automatically update with live information. You can also force an update of the information displayed by clicking **Refresh**.

Chapter 7

Advanced Configuration

- Configuring an Ethernet (wired) interface
- Configuring a wireless interface
- Configuring network security
- Configuring radio settings

Configuring an Ethernet (wired) interface

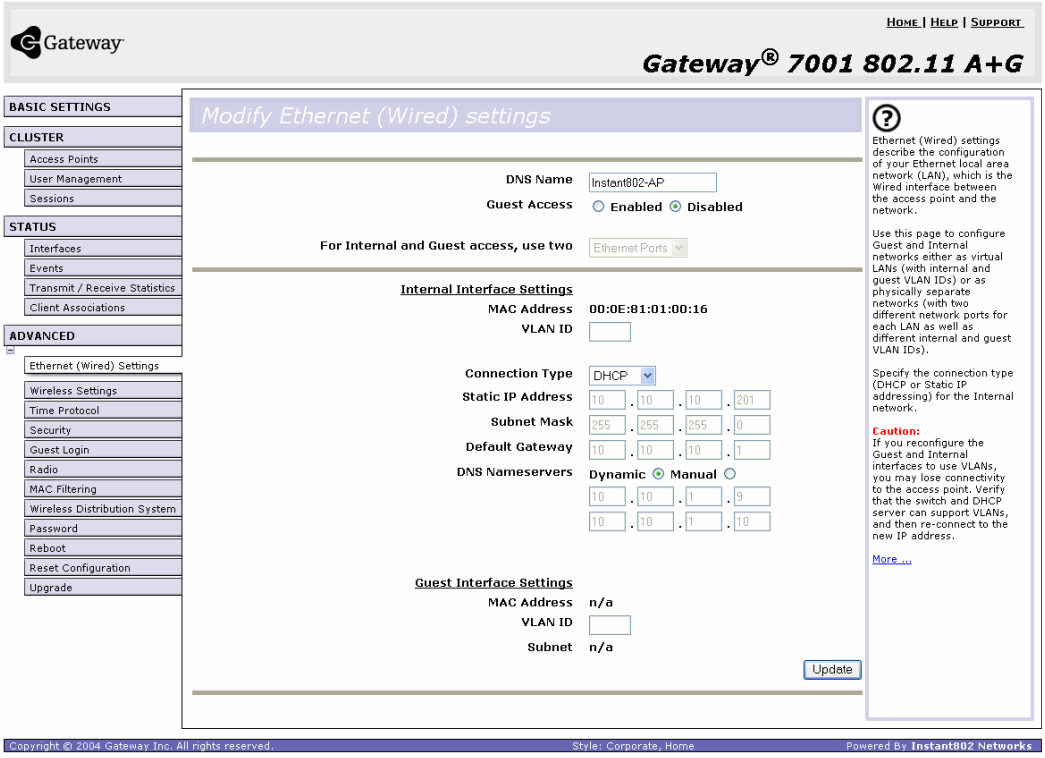
Ethernet (Wired) Settings describe the configuration of your Ethernet local area network (LAN)

Caution

The Ethernet Settings, including Guest Access, are not shared across the cluster. These settings must be configured individually on the Administration pages for each access point. To get to the Administration pages for an access point that is a member of the current cluster, click on its IP Address link on the **Cluster > Access Points** page of the current AP. For more information about which settings are shared by the cluster and which are not, see "Which settings are shared in the cluster configuration and which are not?" on page 43.

Navigating to Ethernet (wired) settings

To set the wired address for an access point, **Advanced > Ethernet (Wired) Settings** on the *Administration* Web page, and update the boxes as described in the following section.



Setting the DNS name

Field	Description
DNS Name	Type a DNS name for the access point in the text box. This is the host name. It may be provided by your ISP or network administrator, or you can provide your own. The rules for system names are: • This name can be up to 20 characters long. • Only letters, numbers and dashes are allowed. • The name must start with a letter and end with either a letter or a number.

Enabling or Disabling Guest Access

You can provide controlled guest access over an isolated network and a secure internal LAN on the same Gateway 7001 Series self-managed AP.

Configuring an internal LAN and a guest network

A *Local Area Network* (LAN) is a communications network covering a limited area, for example, one floor of a building. A LAN connects multiple computers and other network devices like storage and printers.

Ethernet is the most common technology implementing a LAN. Wi-Fi (IEEE) is another popular LAN technology.

The Gateway 7001 Series self-managed AP lets you configure two different LANs on the same access point: one for a secure internal LAN and another for a public guest network with no security and little or no access to internal resources. To configure these networks, you need to provide both Wireless and Ethernet (Wired) settings.

Information on how to configure the Ethernet (Wired) settings is provided in the next sections.

(For information on how to configure the Wireless settings, see "Configuring a wireless interface" on page 74. For an overview of how to set up the guest interface, see "Advanced Configuration" on page 67.)

Enabling or Disabling Guest Access

The Gateway 7001 Series self-managed AP ships with the Guest Access feature disabled by default. If you want to provide guest access on your AP, enable Guest access on the Ethernet (Wired) Settings tab.

Field	Description
Guest Access	By default, the Gateway® 7001 AP ships with Guest Access disabled. • To enable Guest Access, click **Enabled**. • To disable Guest Access, click **Disabled**.

Specifying a physical or virtual Guest network

If you enable Guest Access, you must choose a method of representing both an internal and guest Network on this access point. There are two ways of doing this:

- Physically, by connecting the two LAN ports on the access point to different networks with two different cables, one to the internal LAN and another to a guest network.
- Virtually, by connecting the LAN port on the access point to a tagged port on a VLAN capable switch then defining two different virtual LANs on this *Administration* page. (For more information, see "Advanced Configuration" on page 67).

Choose either physically separate or virtually separate internal and guest LANs as described in the following section.

Field	Description
For Internal and Guest access, use two	Specify either a physically or virtually separate guest network on this access point: ▪ If you connected this access point to two separate networks for a “physically secure” solution, then choose **Ethernet Ports** from the list. (Choosing “Ethernet Ports” here will disable the “VLAN” settings.) ▪ If the access point is using only one physical connection to your internal LAN (extra port is not in use), then choose **VLANs** from the list. (This will enable the “VLAN” settings.)

Caution

If you reconfigure the Guest and Internal interfaces to use VLANs, you may lose connectivity to the access point. First, be sure to verify that the switch and DHCP server you are using can support VLANs per the IEEE 802.1Q standard. After configuring the VLAN on the *Advanced > Ethernet (Wired) Settings* page, physically reconnect the Ethernet cable on the switch to the tagged packet (VLAN) port. Then, re-connect through the Administration Web pages to the new IP address. (If necessary, check with the infrastructure support administrator regarding the VLAN and DHCP configurations.)

Configuring Internal interface Ethernet settings

To configure Ethernet (Wired) settings for the internal LAN, fill in the boxes as described in the following table.

Field	Description
MAC Address	Shows the MAC address for the internal interface for this access point. This is a read only box that you cannot change.
VLAN ID	If you choose to configure internal and guest networks by “VLANs”, this box will be enabled. Provide a number between 1 and 4094 for the internal VLAN. This will cause the access point to send DHCP requests with the VLAN tag. The switch and the DHCP server must support VLAN IEEE 802.1Q frames. The access point must be able to reach the DHCP server. Check with the Administrator regarding the VLAN and DHCP configurations.

Field	Description
Connection Type	You can select “DHCP Client” or “Static IP”. The *Dynamic Host Configuration Protocol* (DHCP) is a protocol specifying how a centralized server can provide network configuration information to clients. A DHCP server “offers” a “lease” to the client system. The information supplied includes the client's IP addresses and net mask plus the address of its DNS servers and gateway. Static IP indicates that all network settings are provided manually. You must provide the IP address for the Gateway 7001 Series self-managed Access Point, its subnet mask, the IP address of the default gateway, and the IP address of at least one DNS nameserver. If you select “DHCP Client”, the Gateway 7001 Series self-managed AP will acquire its IP Address, subnet mask, and DNS and gateway information from the DHCP Servers. Otherwise, if you select “Static IP”, fill in the items described in “Static IP Settings.” **IMPORTANT**: If you do not have a DHCP server on the Internal network and do not plan to use one, the first thing you must do after bringing up the AP is change the Connection Type from DHCP to Static IP. When you change the Connection Type to Static IP, you can either assign a new Static IP Address to the AP or continue using the default address. We recommend assigning a new address so that if later you bring up another Gateway 7001 Series self-managed AP on the same network, the IP addresses for the two APs will be unique. If you need to recover the default Static IP address, you can do so by resetting the AP to the factory defaults as described in “Resetting the configuration” on page 166.
Static IP Address	If you chose “Static IP” as the Connection Type, these boxes will be enabled. Type the Static IP Address in the text boxes.
Subnet Mask	Type the Subnet Mask in the text boxes. You must obtain this information from your ISP or network administrator.
Default Gateway	Type the Default Gateway in the text boxes.
DNS Nameservers	The *Domain Name Service* (DNS) is a system that resolves the descriptive name (domainname) of a network resource (for example, www.gatewayap.com) to its numeric IP address (66.93.138.219). A DNS server is called a Nameserver. There are usually two Nameservers, a Primary and a Secondary. You can choose **Dynamic** or **Manual** mode. ▪ If you choose **Manual**, you should assign static IP addresses manually. ▪ If you choose **Dynamic**, the IP addresses for the DNS servers will be assigned automatically through DHCP. (This option is only available if you specified DHCP for the Connection Type.).

Configuring Guest interface Ethernet settings

To configure Ethernet (Wired) settings for the "Guest" interface, fill in the boxes as described in the following table.

Field	Description
MAC Address	Shows the MAC address for the guest interface for this access point. This is a read-only box that you cannot change.
VLAN ID	If you choose to configure internal and guest networks by "VLANs", this box will be enabled. Provide a number between 1 and 4094 for the guest VLAN.

Updating settings

To apply your changes, click **Update**.

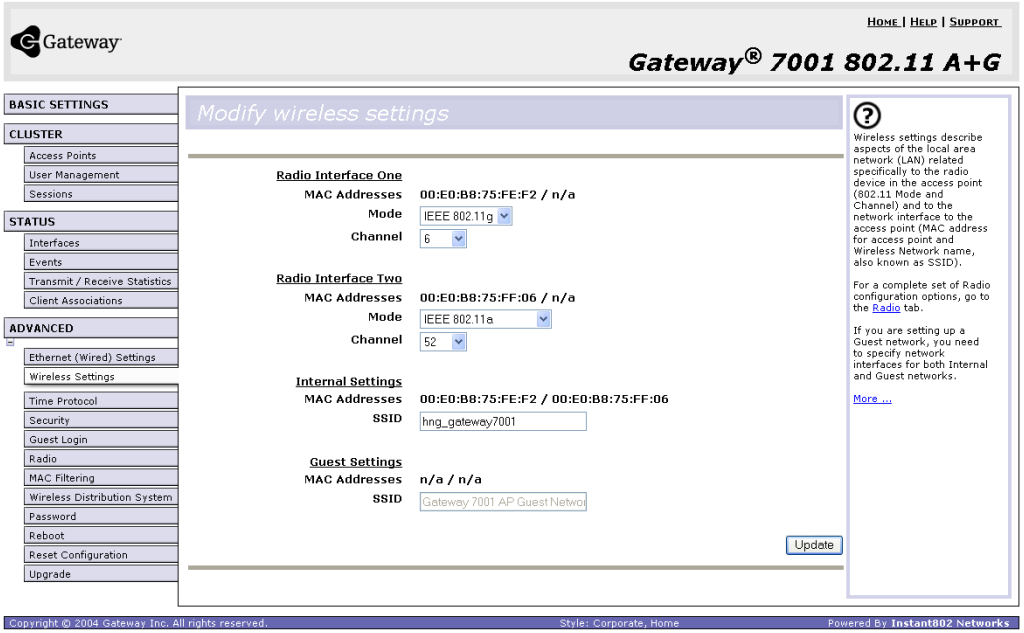
Configuring a wireless interface

Navigating to wireless settings

To set the wireless address for an access point, click **Advanced > Wireless Settings** on the *Administration* Web page, and update the boxes as described in the following section.

Important

The following illustration shows the Wireless settings page for the dual band AP (Gateway 7001 802.11 A+G Wireless Access Point). The *Administration* Web page for the single band AP (Gateway 7001 802.11 G Wireless Access Point) will look slightly different.



Configuring the radio interface

The radio interface lets you set the radio Channel and 802.11 mode as described in the following table.

Important

On the dual band AP (Gateway 7001 802.11 A+G Wireless Access Point), you must configure these radio interface settings for both Radio Interface One and Radio Interface Two.

Field	Description
MAC Addresses (Shown on dual-band AP only)	Indicates the Media Access Control (MAC) addresses for the interface. On the dual band AP only, the MAC addresses for Radio Interface One (Internal/Guest) and Radio Interface Two (Internal/Guest) are shown. A MAC address is a permanent, unique hardware address for any device that represents an interface to the network. The MAC address is assigned by the manufacturer. You cannot change the MAC address. It is provided here for informational purposes as a unique identifier for an interface.
Mode	The Mode defines the Physical Layer (PHY) standard being used by the radio. The Gateway 7001 AP is available in a dual band and single band version. The configuration options for Mode differ depending on which product you have. **Single-Band AP**: For the Single-Band AP, select one of these modes: • IEEE 802.11b • IEEE 802.11g **Dual-Band AP**: For the dual band access point, select a mode for each Radio Interface. For Radio Interface One, select either of these modes: • IEEE 802.11b • IEEE 802.11g For Radio Interface Two, select either of these modes: • IEEE 802.11a • Atheros Turbo 5 GHz (IEEE 802.11a Turbo)
Channel	Select the Channel. The range of channels and the default is determined by the Mode of the radio interface. The *Channel* defines the portion of the radio spectrum the radio uses for transmitting and receiving. Each mode offers a number of channels, dependent on how the spectrum is licensed by national and international authorities such as the Federal Communications Commission (FCC) or the International Telecommunication Union (ITU-R). The default is **Auto**, which picks the least busy channel at startup time, out of the allowed channels.

Configuring internal LAN wireless settings

The internal settings describe the MAC Address (read-only) and Network Name (also known as the SSID) for the internal Wireless LAN (WLAN) as described in the following section.

Field	Description
MAC Address	Shows the MAC address for internal interface for this access point. This is a read only box that you cannot change. Although this access is point is physically a single device, it is represented on the network as two nodes each with a unique MAC Address. This is accomplished by using two different Basic Service Set Identifiers (BSSIDs) for a single access point. The MAC address shown for the internal access point is the BSSID for the internal interface. For the dual-band AP (Gateway 7001 802.11 A+G Wireless Access Point), two MAC addresses are shown: one for each radio on the internal interface.
SSID	Type the SSID for the internal WLAN. The *Service Set Identifier* (SSID) is an alphanumeric string of up to 32 characters that uniquely identifies a wireless local area network. It is also referred to as the Network Name. There are no restrictions on the characters that may be used in an SSID.

Configuring guest network wireless settings

The Guest Settings describe the MAC Address (read-only) and wireless network name (SSID) for the guest network as described in the following section. Configuring an access point with two different network names (SSIDs) lets you leverage the guest interface feature on the Gateway 7001 Series self-managed AP. For more information, see "Advanced Configuration" on page 67.

Field	Description
MAC Address	Shows the MAC address for guest interface for this access point. This is a read only box that you cannot change. Although this access is point is physically a single device, it is represented on the network as two nodes each with a unique MAC Address. This is accomplished by using two different Basic Service Set Identifiers (BSSIDs) for a single access point. The MAC address shown for the guest access point is the BSSID for the guest interface. For the dual-band AP (Gateway 7001 802.11 A+G Wireless Access Point), two MAC addresses are shown: one for each Radio on the internal interface.

Field	Description
SSID	Type the SSID for the internal WLAN. The *Service Set Identifier* (SSID) is an alphanumeric string of up to 32 characters that uniquely identifies a wireless local area network. It is also referred to as the Network Name. There are no restrictions on the characters that may be used in an SSID. For the guest network, provide an SSID that is different from the internal SSID and easily identifiable as the guest network.

Updating settings

To apply your changes, click **Update**.

Enabling a network time protocol server

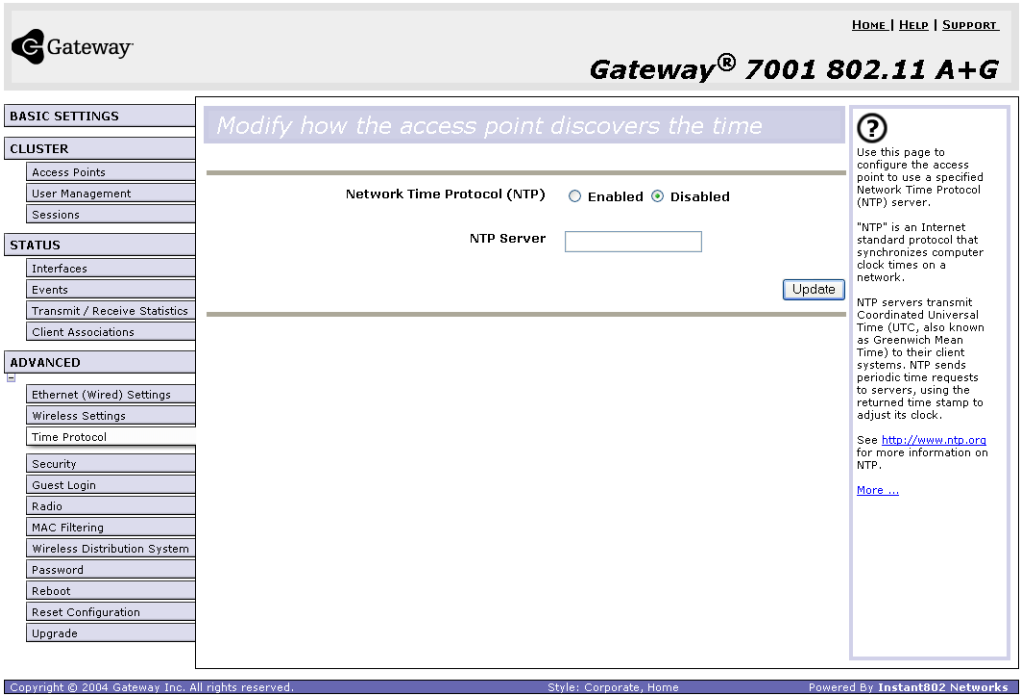
The *Network Time Protocol* (NTP) is an Internet standard protocol that synchronizes computer clock times on your network. NTP servers transmit *Coordinated Universal Time* (UTC, also known as *Greenwich Mean Time*) to their client systems. NTP sends periodic time requests to servers, using the returned time stamp to adjust its clock.

The timestamp will be used to indicate the date and time of each event in log messages.

See http://www.ntp.org for more general information on NTP.

Navigating to time protocol settings

To enable an NTP server, click **Advanced > Time Protocol** on the Administration Web page. The *Modify how the access point discovers the time* screen opens. Update the boxes as described in the following section.



Enabling or disabling a network time protocol (NTP) server

To configure your access point to use a network time protocol (NTP) server, first enable the use of NTP, then select the NTP server you want to use. (To shut down NTP service on the network, disable NTP on the access point.)

Field	Description
Network Time Protocol	NTP provides a way for the access point to obtain and maintain its time from a server on the network. Using an NTP server gives your AP the ability to provide the correct time of day in log messages and session information. (See http://www.ntp.org for more general information on NTP.) Choose to either enable or disable use of a network time protocol (NTP) server: • Enabled • Disabled
NTP Server	If NTP is enabled, select the NTP server you want to use. You can specify the NTP server by host name or IP address, although using the IP address is not recommended as these can change more readily.

Updating settings

To apply your changes, click **Update**.

Configuring network security

Understanding security issues on wireless networks

Wireless mediums are inherently less secure than wired mediums. For example, an Ethernet NIC transmits its packets over a physical medium such as coaxial cable or twisted pair. A wireless NIC broadcasts radio signals over the air allowing a wireless LAN to be easily tapped without physical access or sophisticated equipment. A hacker equipped with a laptop, a wireless NIC, and a bit of knowledge can easily attempt to compromise your wireless network. One does not even need to be within normal range of the access point. By using a sophisticated antenna on the client, a hacker may be able to connect to the network from many miles away.

The Gateway 7001 Series self-managed AP provides a number of authentication and encryption schemes to make sure that your wireless infrastructure is accessed only by the intended users. The details of each security mode are described in the following sections.

How do I know which security mode to use?

In general, we recommend that on your internal network you use the most robust security mode that is feasible in your environment. When configuring security on the access point, you first must choose the security mode, then in some modes an authentication algorithm, and whether to allow clients not using the specified security mode to associate.

Wi-Fi Protected Access (WPA) with Remote Authentication Dial-In User Service (RADIUS) using the CCMP (AES) encryption algorithm provides the best data protection available and is clearly the best choice if all client stations are equipped with WPA supplicants. However, backward compatibility or interoperability issues with clients or even with other access points may require that you configure WPA with RADIUS with a different encryption algorithm or choose one of the other security modes.

That said, however, security may not be as much of a priority on some types of networks. If you are simply providing internet and printer access, as on a guest network, plain text mode (no security) may be the appropriate choice. To prevent clients from accidentally discovering and connecting to your network, you can disable the broadcast SSID so that your network name is not advertised. If the network is sufficiently isolated from access to sensitive information, this may offer enough protection in some situations. This level of protection is the only one offered for guest networks, and also may be the right convenience trade-off for other scenarios where the priority is making it as easy as possible for clients to connect. (See “Does Prohibiting the Broadcast SSID Enhance Security?” on page 86.)

Following is a brief discussion of what factors make one mode more secure than another, a description of each mode offered, and when to use each mode.

Comparison of security modes for key management, authentication, and encryption algorithms

The three major factors that determine the effectiveness of a security protocol are:

- How the protocol manages keys
- Presence or absence of integrated user authentication in the protocol
- Encryption algorithm or formula the protocol uses to encode/decode the data

Following is a list of the security modes available on the Gateway 7001 Series self-managed AP along with a description of the key management, authentication, and encryption algorithms used in each mode. We include some suggestions as to when one mode might be more appropriate than another.

When to use plain text

Plain text mode by definition provides no security. In this mode, the data is not encrypted but rather sent as plain text across the network. No key management, data encryption, or user authentication is used.

Recommendations

Plain text mode is **not recommended** for regular use on the internal network because it is not secure.

Plain text mode is the only mode in which you can run the guest network, which is by definition an unsecure LAN always virtually or physically separated from any sensitive information on the internal LAN.

Therefore, use plain text mode on the guest network, and on the internal network for initial setup, testing, or problem solving only.

For information on how to configure plain text mode, see "Plain-text" on page 88.

When to use static WEP

Static *Wired Equivalent Privacy* (WEP) is a data encryption protocol for 802.11 wireless networks. All wireless stations and access points on the network are configured with a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared Key for data encryption.

Key Management	Encryption Algorithm	User Authentication
Static WEP uses a fixed key that is provided by the administrator. WEP keys are indexed in different slots (up to four on the Gateway 7001 Series self-managed AP). The client stations must have the same key indexed in the same slot to access data on the access point.	An RC4 stream cipher is used to encrypt the frame body and cyclic redundancy checking (CRC) of each 802.11 frame.	If you set the Authentication Algorithm to Shared Key, this protocol provides a rudimentary form of user authentication. However, if the Authentication Algorithm is set to "Open System", no authentication is performed. If the algorithm is set to "Both", only WEP clients are authenticated.

Recommendations

Static WEP was designed to provide security equivalent of sending unencrypted data through an Ethernet connection, however it has major flaws and it does not provide even this intended level of security.

Therefore, Static WEP is not recommended as a secure mode. The only time to use Static WEP is when interoperability issues make it the only option available to you and you are not concerned with the potential of exposing the data on your network.

For information on how to configure Static WEP security mode, see "Static WEP" on page 89.

When to use IEEE 802.1x

IEEE 802.1x is the standard for passing the Extensible Authentication Protocol (EAP) over an 802.11 wireless network using a protocol called EAP Encapsulation Over LANs (EAPOL). This is a newer, more secure standard than Static WEP.

While parts of 802.1x are indeed standard, it uses port control with dynamically varying encryption keys that can be automatically updated over the network with the Extensible Authentication Protocol (EAP) to enable user, not machine, authentication. To make all this happen, 802.1x uses RADIUS servers.

Key Management	Encryption Algorithm	User Authentication
IEEE 802.1x provides dynamically generated keys that are periodically refreshed. There are different Unicast keys for each station.	An RC4 stream cipher is used to encrypt the frame body and cyclic redundancy checking (CRC) of each 802.11 frame. (This is the same encryption algorithm as is used for Static WEP.)	IEEE 802.1x mode supports a variety of authentication methods, like certificates, Kerberos, and public key authentication with a RADIUS server. You have a choice of using the Gateway 7001 Series self-managed AP embedded RADIUS server or an external RADIUS server. The embedded RADIUS server supports Protected EAP (PEAP) and MSCHAP V2.

Recommendations

IEEE 802.1x mode is a better choice than Static WEP because keys are dynamically generated and changed periodically. However, the encryption algorithm used is the same as that of Static WEP and is therefore not as reliable as the more advanced encryption methods such as TKIP and CCMP (AES) used in Wi-Fi Protected Access (WPA).

Additionally, compatibility issues may be cumbersome because of the variety of authentication methods supported and the lack of a standard implementation method. For this reason, if you do use IEEE 802.1x, we suggest using it with the embedded RADIUS server.

Therefore, IEEE 802.1x mode is not as secure a solution as Wi-Fi Protected Access (WPA). If you cannot use Wi-Fi Protected Access (WPA) because some of your client stations do not have WPA, then a better solution than using IEEE 802.1x mode is to use WPA with RADIUS mode instead and click **Allow non-WPA IEEE 802.1x clients** to allow non-WPA clients. This way, you get the benefit of IEEE 802.1x key management for non-WPA clients along with even better data protection of TKIP and CCMP (AES) key management and encryption algorithms for your WPA clients.

For information on how to configure IEEE 802.1x security mode, see "IEEE 802.1x" on page 93.

When to use WPA with RADIUS

Wi-Fi Protected Access (WPA) with *Remote Authentication Dial-In User Service* (RADIUS) is a Wi-Fi Alliance subset of IEEE 802.11i, which includes Temporal Key Integrity Protocol (TKIP), Counter mode/ CBC-MAC Protocol (CCMP) Advanced Encryption Standard (AES), and 802.1x mechanisms. This mode requires the use of a RADIUS server to authenticate users. WPA with RADIUS provides the best security available for wireless networks.

Key Management	Encryption Algorithm	User Authentication
WPA with RADIUS provides dynamically-generated keys that are periodically refreshed. There are different Unicast keys for each station.	• Temporal Key Integrity Protocol (TKIP) • Counter mode/CBC-MAC Protocol (CCMP) Advanced Encryption Standard (AES)	Remote Authentication Dial-In User Service (RADIUS) You have a choice of using the Gateway 7001 Series self-managed AP embedded RADIUS server or an external RADIUS server. The embedded RADIUS server supports Protected EAP (PEAP) and MSCHAP V2.

Recommendations

WPA with RADIUS mode is the **recommended mode**. The CCMP (AES) and TKIP encryption algorithms used with WPA modes are far superior to the RC4 algorithm used for Static WEP or IEEE 802.1x modes. Therefore, CCMP (AES) or TKIP should be used whenever possible. All WPA modes allow you to use these encryption schemes, so WPA security modes are recommended above the others when using WPA is an option.

Additionally, this mode (WPA with RADIUS) incorporates a RADIUS server for user authentication which gives it an edge over WPA-PSK.

Use the following guidelines for choosing options within the WPA with RADIUS security mode:

- The best security you can have to date on a wireless network is WPA with RADIUS using CCMP (AES) encryption algorithm. AES is a symmetric 128-bit block data encryption technique that works on multiple layers of the network. It is the most effective encryption system currently available for wireless networks. If all clients or other APs on the network are WPA/CCMP compatible, use this encryption algorithm.
- The second best choice is WPA with RADIUS with the encryption algorithm set to "Both" (that is, both TKIP and CCMP). This lets WPA client stations without CCMP associate, uses TKIP for encrypting Multicast and Broadcast frames, and lets you select whether to use CCMP or TKIP for Unicast (AP-to-single-station) frames. This WPA configuration allows more interoperability, at the expense of some security. Client stations that support CCMP can use it for their Unicast frames. If you encounter AP-to-station interoperability problems with the "Both" encryption algorithm setting, then you will need to select TKIP instead.
- The third best choice is WPA with RADIUS with the encryption algorithm set to TKIP. Some clients have interoperability issues with CCMP and TKIP enabled at same time. If you encounter this problem, then choose TKIP as the encryption algorithm. This is the standard WPA mode, and most interoperable mode with client wireless software security features. TKIP is the only encryption algorithm that is being tested in Wi-Fi WPA certification.

Important

If there are older client stations on your network that do not support WPA, you can configure WPA with RADIUS (with Both, CCMP, or TKIP) and check the **Allow non-WPA IEEE 802.1x clients** checkbox to allow non-WPA clients. This way, you get the benefit of IEEE 802.1x key management for non-WPA clients along with even better data protection of TKIP and CCMP (AES) key management and encryption algorithms for your WPA clients.

A typical scenario is that one is upgrading a current 802.1x network to use WPA. You might have a mix of clients, in which some new clients that support WPA and some older ones that do not support WPA. You might even have other access points on the network that support only 802.1x and some that support WPA with RADIUS. For as long as this mix persists, use the **Allow non-WPA IEEE 802.1x clients** option When all the stations have been upgraded to use WPA, you should disable the **Allow non-WPA IEEE 802.1x clients** option.

For information on how to configure WPA with RADIUS security mode, see "WPA with RADIUS" on page 95.

When to use WPA-PSK

Wi-Fi Protected Access (WPA) with *Pre-Shared Key* (PSK) is a Wi-Fi Alliance subset of IEEE 802.11i, which includes Temporal Key Integrity Protocol (TKIP) and 802.1x mechanisms. This mode offers the same encryption algorithms as WPA with RADIUS but without the ability to integrate a RADIUS server for user authentication.

Key Management	Encryption Algorithm	User Authentication
WPA-PSK provides dynamically-generated keys that are periodically refreshed. There are different Unicast keys for each station.	• Temporal Key Integrity Protocol (TKIP) • Counter mode/CBC-MAC Protocol (CCMP) Advanced Encryption Standard (AES)	The use of a Pre-Shared (PSK) key provides user authentication similar to that of shared keys in WEP.

Recommendations

WPA-PSK is not recommended for use with the Gateway 7001 Series self-managed AP when WPA with RADIUS is an option.

We recommend that you use WPA with RADIUS mode instead, unless you have interoperability issues that prevent you from using this mode.

For example, some devices on your network may not support WPA with EAP talking to a RADIUS server. Embedded printer servers or other small client devices with very limited space for implementation may not support RADIUS. For such cases, we recommend that you use WPA-PSK.

For information on how to configure WPA-PSK security mode, see "WPA-PSK" on page 97.

Does Prohibiting the Broadcast SSID Enhance Security?

You can suppress (prohibit) this broadcast to discourage stations from automatically discovering your access point. When the AP's broadcast SSID is suppressed, the network name will not be displayed in the List of Available Networks on a client station. Instead, the client must have the exact network name configured before it will be able to connect.

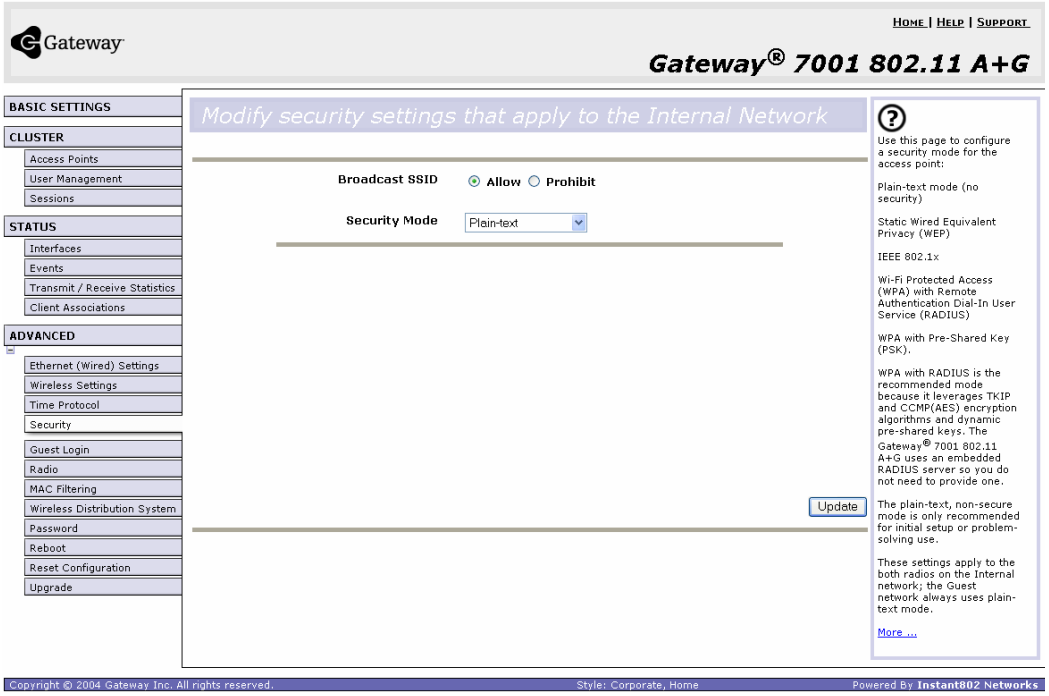
Disabling the broadcast SSID is sufficient to prevent clients from accidentally connecting to your network, but it will not prevent even the simplest of attempts by a hacker to connect, or monitor plain text traffic.

This offers a very minimal level of protection on an otherwise exposed network (such as a guest network) where the priority is making it easy for clients to get a connection and where no sensitive information is available.

(See also "Guest Network" on page 88.)

Navigating to security settings

To set the security mode, click **Advanced > Security** on the Administration Web page. The *Modify security settings that apply to the internal network* screen opens. Update the boxes as described in the following section.



Configuring security settings

The following configuration information explains how to configure security modes on the access point.

Keep in mind that each wireless client that wants to exchange data with the access point must be configured with the same security mode and encryption key settings used on the access point.

On a dual-band AP, these Security Settings apply to both radios.

Important

Security modes other than plain-text apply only to configuration of the internal network. On the guest network, you can use only plain-text mode. (For more information about guest networks, see "Setting up Guest Access" on page 99.)

Broadcast SSID and Security Mode

To configure security on the access point, select a security mode and fill in the related boxes as described in the following table. (Note you can also allow or prohibit the Broadcast SSID as an extra precaution as mentioned in the following section.)

Field	Description
Broadcast SSID	Select the Broadcast SSID setting by clicking the **Allow** or **Prohibit** option. By default, the access point broadcasts the *Service Set Identifier* (SSID) in its beacon frames. Suppress this broadcast to discourage stations from automatically discovering your access point. You can suppress (prohibit) this broadcast to discourage stations from automatically discovering your access point. When the AP's broadcast SSID is suppressed, the network name will not be displayed in the List of Available Networks on a client station. Instead, the client must be configured with the exact network before it will be able to connect.
Security Mode	Select the Security Mode. Select one of the following: • **Plain-text** • **Static WEP** • **IEEE 802.1x** • **WPA with RADIUS** • **WPA-PSK** Security modes other than plain-text apply only to configuration of the internal network. On the guest network, you can use only plain-text mode. (For more information, see "Setting up Guest Access" on page 99.)

Plain-text

Plain Text means any data transferred to and from the Gateway 7001 Series self-managed AP is not encrypted.

There are no further options for plain-text mode.

Plain text mode can be useful during initial network configuration or for problem solving, but it is not recommended for regular use on the internal network because it is not secure.

Guest Network

Plain text mode is the only mode in which you can run the guest network, which is by definition an unsecure LAN always virtually or physically separated from any sensitive information on the internal LAN.

The absence of security on the Guest AP is designed to make it as easy as possible for guests to get a connection without having to program any security settings in their clients.

For a minimum level of protection on a guest network, you can choose to suppress (prohibit) the broadcast of the SSID (network name) to discourage client stations from automatically discovering your access point. (See also "Does Prohibiting the Broadcast SSID Enhance Security?" on page 86.)

(For more about the guest network, see "Setting up Guest Access" on page 99.)

Static WEP

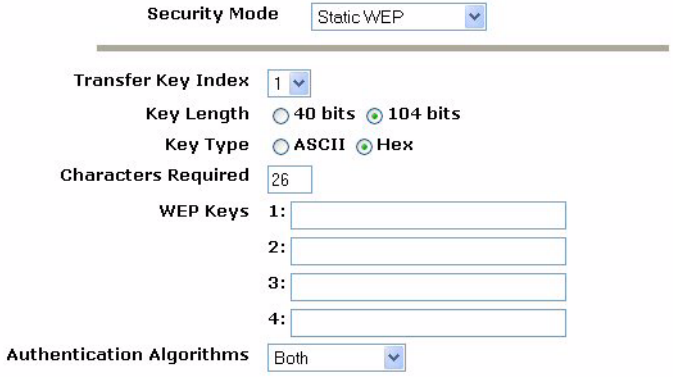
Wired Equivalent Privacy (WEP) is a data encryption protocol for 802.11 wireless networks. All wireless stations and access points on the network are configured with a static 64-bit (40-bit secret key + 24-bit initialization vector (or IV)), or 128-bit (104-bit secret key + 24-bit IV) Shared Key for data encryption.

You cannot mix 64-bit and 128-bit WEP keys between the access point and its client stations.

Static WEP is not the most secure mode available, but it offers more protection than plain-text mode as it does prevent an outsider from easily sniffing out unencrypted wireless traffic. (For more secure modes, see "IEEE 802.1x" on page 93, "WPA with RADIUS" on page 95, or "WPA-PSK" on page 97.) WEP encrypts data moving across the wireless network based on a static key. (The encryption algorithm is a "stream" cipher called RC4.)

The access point uses a key to transmit data to the client stations. Each client station must use that same key to decrypt data it receives from the access point.

Client stations can use different keys to transmit data to the access point. (Or they can all use the same key, but this is less secure because it means one station can decrypt the data being sent by another.) If you selected "Static WEP" security mode, provide the following on the access point settings:



Field	Description
Transfer Key Index	Select a key index from the list. Key indexes 1 through 4 are available. The default is 1. The *Transfer Key Index* indicates which WEP key the access point will use to encrypt the data it transmits.
Key Length	Specify the length of the key by clicking one of the options: • 64 bits • 128 bits
Key Type	Select the key type by clicking one of the options: • ASCII • Hex
Characters Required	Indicates the number of characters required in the WEP key. The number of characters required updates automatically based on how you set Key Length and Key Type.
WEP Keys	You can specify up to four WEP keys. In each text box, type a string of characters for each key. If you selected **ASCII**, type any combination of numbers and letters 0-9, a-z, and AZ. If you selected **HEX**, type hexadecimal digits (any combination of 0-9 and a-f or A-F). Use the same number of characters for each key as specified in the **Characters Required** box. These are the RC4 WEP keys shared with the stations using the access point. Each client station must be configured to use one of these same WEP keys in the same slot as specified here on the AP. (See "Rules to Remember for Static WEP" on page 91.)

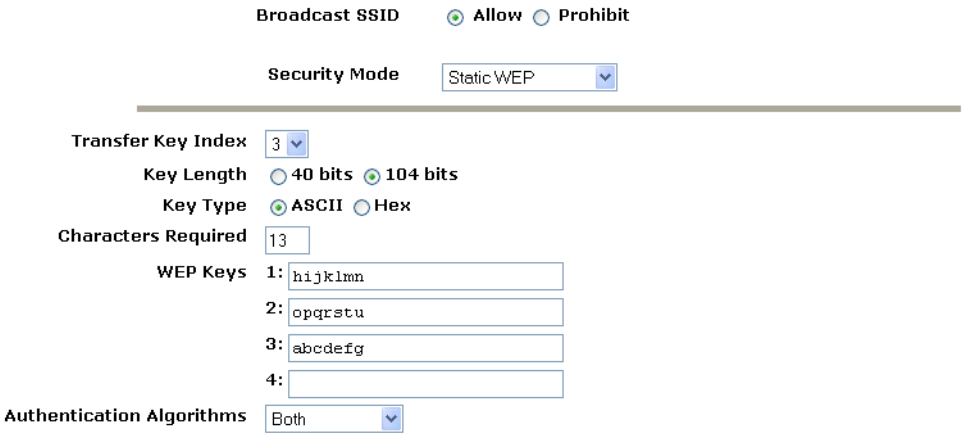
Field	Description
Authentication Algorithm	The authentication algorithm defines the method used to determine whether a client station is allowed to associate with an access point when static WEP is the security mode. Specify the authentication algorithm you want to use by choosing one of the following from the list: • **Open System** • **Shared Key** • **Both** **Open System** authentication lets any client station associate with the access point whether that client station has the correct WEP key or not. This algorithm is also used in plain text, IEEE 802.1x, and WPA modes. When the authentication algorithm is set to **Open System**, any client can associate with the access point. Note that just because a client station is allowed to associate does not ensure it can exchange traffic with an access point. A station must have the correct WEP key to be able to successfully access and decrypt data from an access point, and to transmit readable data to the access point. **Shared Key** authentication requires the client station to have the correct WEP key in order to associate with the access point. When the authentication algorithm is set to **Shared Key**, a station with an incorrect WEP key will not be able to associate with the access point. **Both** is the default. When the authentication algorithm is set to **Both**: • Client stations configured to use WEP in shared key mode must have a valid WEP key in order to associate with the access point. • Client stations configured to use WEP as an open system (shared key mode not enabled) will be able to associate with the access point even if they do not have the correct WEP key.

Rules to Remember for Static WEP

- All client stations must have the Wireless LAN (WLAN) security set to WEP and all clients must have one of the WEP keys specified on the AP in order to de-crypt AP-to-station data transmissions.
- The AP must have all keys used by clients for station-to-AP transmit so that it can de-crypt the station transmissions.
- The same key most occupy the same slot on all nodes (AP and clients). For example if the AP defines abc123 key as WEP key 3, then the client stations must define that same string as WEP key 3.
- On some wireless client software (like Funk Odyssey), you can configure multiple WEP keys and define a client station transfer key index, then set the stations to encrypt the data they transmit using different keys. This ensures that neighboring APs cannot decrypt each other's transmissions.

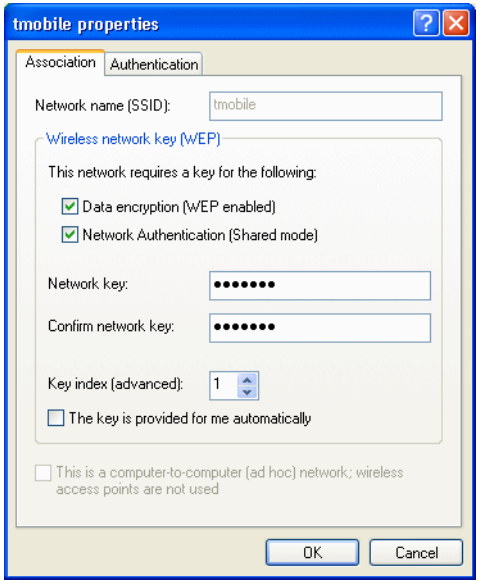
Example of Using Static WEP

For a simple example, suppose you configure three WEP keys on the access point. In our example, the Transfer Key Index for the AP is set to **3**. This means that the WEP key in slot 3 is the key the access point will use to encrypt the data it sends.



You must then set all client stations to use WEP and provide each client with one of the slot/key combinations you defined on the AP.

For this example, we will set WEP Key index to **1** on a Windows client.



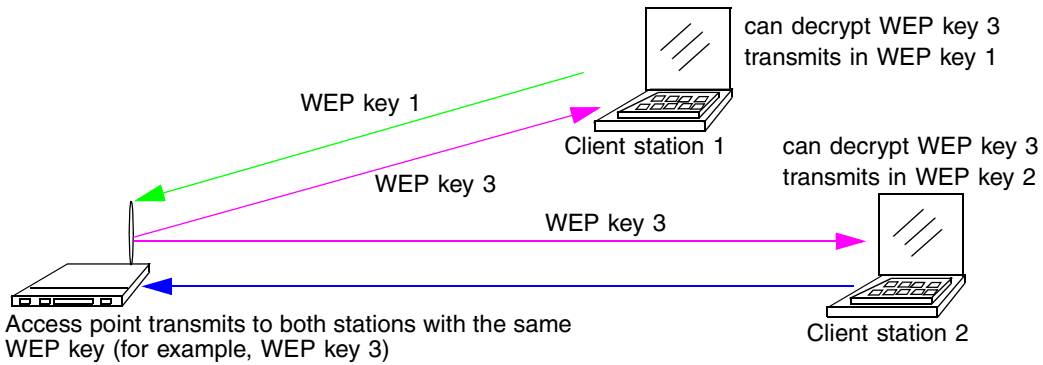
If you have a second client station, that station also needs to have one of the WEP keys defined on the AP. You could give it the same WEP key you gave to the first station. Or for a more secure solution, you could give the second station a different WEP key (key 2, for example) so that the two stations cannot decrypt each other's transmissions.

Static WEP with Transfer Key Indexes on Client Stations

Some Wireless client software (like Funk Odyssey) lets you configure multiple WEP keys and set a transfer index on the client station, then you can specify different keys to be used for station-to-AP transmissions. (The standard Windows wireless client software does not allow you to do this.)

To build on our example, using Funk Odyssey client software you could give each of the clients WEP key 3 so that they can decode the AP transmissions with that key and also give client 1 WEP key 1 and set this as its transfer key. You could then give client 2 WEP key 2 and set this as its transfer key index.

The following figure illustrates the dynamics of the AP and two client stations using multiple WEP keys and a transfer key index.



IEEE 802.1x

IEEE 802.1x is a standard for network access control. It involves passing the Extensible Authentication Protocol (EAP) over IEEE 802.11 LANs using a protocol called EAP Encapsulation Over LANs (EAPOL).

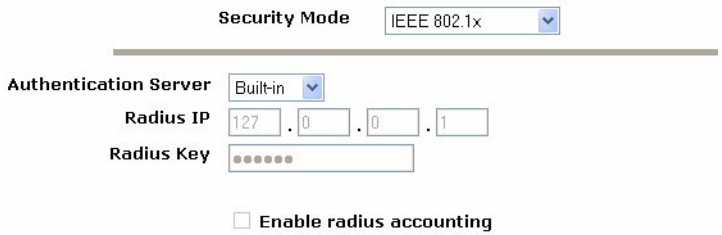
This mode requires the use of a RADIUS server to authenticate users, and configuration of user accounts through the **Cluster > User Management** tab.

The access point requires a RADIUS server capable of EAP, such as the Microsoft Internet Authentication Server or the Gateway 7001 Series self-managed AP internal authentication server. To work with Windows clients, the authentication server must support Protected EAP (PEAP) and MSCHAP V2.

When configuring IEEE 802.1x mode, you have a choice of whether to use the embedded RADIUS server or an external RADIUS server that you provide. The Gateway 7001 Series self-managed AP embedded RADIUS server supports Protected EAP (PEAP) and MSCHAP V2.

If you use your own RADIUS server, you have the option of using any of a variety of authentication methods that the IEEE 802.1x mode supports, including certificates, Kerberos, and public key authentication. Keep in mind, however, that the client stations must be configured to use the same authentication method being used by the access point.

If you selected "IEEE 802.1x" Security Mode, provide the following:



Field	Description
Authentication Server	Select one of the following from the list: ▪ **Built-in** - To use the authentication server provided with the Gateway 7001 Series self-managed AP. If you choose this option, you do not have to provide the Radius IP and Radius Key (they are automatically provided). ▪ **External** - To use an external authentication server. If you choose this option you must supply the Radius IP and Radius Key of the server you want to use.
Radius IP	Type the Radius IP in the text box. The *Radius IP* is the IP address of the RADIUS server. The Gateway 7001 Series self-managed AP internal authentication server is **127.0.0.1**. This will be provided automatically if you selected the built-in authentication server. For more information, see "Managing User Accounts" on page 55.
Radius Key	Type the Radius Key in the text box. The *Radius Key* is the shared secret key for the RADIUS server. The text you type will be displayed as "*" characters to prevent others from seeing the RADIUS key as you type. The Gateway 7001 Series self-managed AP internal authentication server is "secret." This will be provided automatically if you selected the built-in authentication server. This value is never sent over the network.

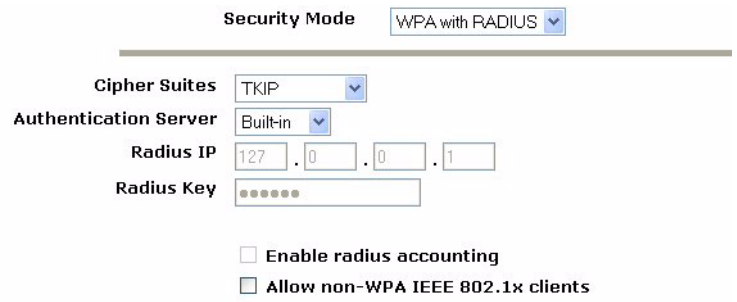
Field	Description
Enable RADIUS Accounting	Click **Enable RADIUS Accounting** if you want to track and measure the resources a particular user has consumed such as system time, amount of data transmitted and received, and so on.

WPA with RADIUS

Wi-Fi Protected Access (WPA) with *Remote Authentication Dial-In User Service* (RADIUS) is a Wi-Fi Alliance subset of IEEE 802.11i, which includes Temporal Key Integrity Protocol (TKIP), Counter mode/ CBC-MAC Protocol (CCMP) Advanced Encryption Standard (AES), and 802.1x mechanisms. This mode requires the use of a RADIUS server to authenticate users.

When configuring WPA with RADIUS mode, you have a choice of whether to use the embedded RADIUS server or an external RADIUS server that you provide. The Gateway 7001 Series self-managed AP embedded RADIUS server supports Protected EAP (PEAP) and MSCHAP V2.

If you selected **WPA with RADIUS** security mode, provide the following:



Field	Description
Cipher Suites	Select the cipher you want to use from the list: • TKIP • CCMP (AES) • Both **Temporal Key Integrity Protocol** (TKIP) is the default. **TKIP** provides a more secure encryption solution than WEP keys. The TKIP process more frequently changes the encryption key used and better ensures that the same key will not be re-used to encrypt data (a weakness of WEP). TKIP uses a 128-bit “temporal key” shared by clients and access points. The temporal key is combined with the client's MAC address and a 16-octet initialization vector to produce the key that will encrypt the data. This ensures that each client station uses a different key to encrypt data. TKIP uses RC4 to perform the encryption, which is the same as WEP. But TKIP changes temporal keys every 10,000 packets and distributes them, thereby greatly improving the security of the network. **Counter mode/CBC-MAC Protocol** (CCMP) is an encryption method for IEEE 802.11i that uses the Advanced Encryption Algorithm (AES). It uses a CCM combined with Cipher Block Chaining Counter mode (CBC-CTR) and Cipher Block Chaining Message Authentication Code (CBC-MAC) for encryption and message integrity. When the authentication algorithm is set to **Both**, both TKIP and AES clients can associate with the access point. Client stations configured to use WPA with RADIUS must have one of the following to be able to associate with the AP: • A valid TKIP RADIUS IP address and valid shared Key • A valid CCMP (AES) IP address and valid shared Key Clients not configured to use WPA-PSK will not be able to associate with AP. **Both** is the default. When the authentication algorithm is set to **Both**, client stations configured to use WPA with RADIUS must have one of the following: • A valid TKIP RADIUS IP address and RADIUS Key • A valid CCMP (AES) IP address and RADIUS Key
Authentication Server	Select one of the following from the list: ▪ **Built-in** - To use the authentication server provided with the Gateway 7001 Series self-managed AP. If you choose this option, you do not have to provide the Radius IP and Radius Key (they are automatically provided). ▪ **External** - To use an external authentication server. If you choose this option you must supply a Radius IP and Radius Key of the server you want to use.

Field	Description
Radius IP	Type the Radius IP in the text box. The *Radius IP* is the IP address of the RADIUS server. The RADIUS IP address for the Gateway 7001 Series self-managed AP internal authentication server is **127.0.0.1**. This will be provided automatically if you selected the built-in authentication server. For information on setting up user accounts, see "Managing User Accounts" on page 55.
Radius Key	Type the Radius Key in the text box. The *Radius Key* is the shared secret key for the RADIUS server. The text you type will be displayed as "*" characters to prevent others from seeing the RADIUS key as you type. The Gateway 7001 Series self-managed AP internal authentication server key is "secret." This will be provided automatically if you selected the built-in authentication server. This value is never sent over the network.
Key Type	Select the key type by clicking one of the options: • ASCII • HEX
Enable RADIUS Accounting	Click **Enable RADIUS Accounting** if you want to enforce authentication for WPA client stations with user names and passwords for each station.
Allow non-WPA Clients	Click **Allow non-WPA clients** if you want to let non-WPA (802.11), unauthenticated client stations use this access point.

WPA-PSK

Wi-Fi Protected Access (WPA) with *Pre-Shared Key* (PSK) is a Wi-Fi Alliance subset of IEEE 802.11i, which includes Temporal Key Integrity Protocol (TKIP), Advanced Encryption Algorithm (AES), Counter mode/CBC-MAC Protocol (CCMP) 802.1x mechanisms. PSK employs a pre-shared key. This is used for an initial check of credentials only.

If you selected "WPA-PSK" Security Mode, provide the following:

Field	Description
Cipher Suites	Select the cipher you want to use from the list: • TKIP • CCMP (AES) • Both **Temporal Key Integrity Protocol** (TKIP) is the default. **TKIP** provides a more secure encryption solution than WEP keys. The TKIP process more frequently changes the encryption key used and better ensures that the same key will not be re-used to encrypt data (a weakness of WEP). TKIP uses a 128-bit “temporal key” shared by clients and access points. The temporal key is combined with the client's MAC address and a 16-octet initialization vector to produce the key that will encrypt the data. This ensures that each client station uses a different key to encrypt data. TKIP uses RC4 to perform the encryption, which is the same as WEP. But TKIP changes temporal keys every 10,000 packets and distributes them, thereby greatly improving the security of the network. **Counter mode/CBC-MAC Protocol** (CCMP) is an encryption method for IEEE 802.11i that uses the Advanced Encryption Algorithm (AES). It uses a CCM combined with Cipher Block Chaining Counter mode (CBC-CTR) and Cipher Block Chaining Message Authentication Code (CBC-MAC) for encryption and message integrity. **Both** is where both TKIP and AES clients can associate with the access point. WPA clients must have one of the following to be able to associate with the AP: • A valid TKIP key • A valid CCMP (AES) key Clients not configured to use WPA-PSK will not be able to associate with AP.
Key	The *Pre-shared Key* is the shared secret key for WPA-PSK. Type a string of at least 8 characters to a maximum of 63 characters.

Updating settings

To apply your changes, click **Update**.

Setting up Guest Access

Out-of-the-box guest interface features allow you to configure the Gateway 7001 Series self-managed AP for controlled guest access to an isolated network. You can configure the same access point to broadcast and function as two different wireless networks: a secure *Internal* LAN and a public *Guest* network.

Guest clients can access the guest network without a user name or password. When guests log in, they see a guest welcome screen (also known as a *captive portal*).

Understanding the guest interface

You can define unique parameters for guest connectivity and isolate guest clients from other more sensitive areas of the network. No security is provided on the guest network and only plain-text security mode is allowed.

Simultaneously, you can configure a secure internal network (using the same access point as your guest interface) that provides full access to protected information behind a firewall and requires secure logins or certificates for access.

You can configure a Gateway 7001 Series self-managed AP for the guest interface in one of two ways:

- Connect the access point to a separate network using the extra, dedicated guest network port on the AP. This provides a physically secure solution that does not require VLAN support. (For details on how to set up this type of guest interface, see "Configuring a physically separate guest network" on page 100.)
- Configure the access point using a single network with VLANs by setting up the guest interface configuration options on the Administration Web pages for the Gateway 7001 Series self-managed AP. (For details on how to set up this type of guest interface, see "Configuring a guest network on a virtual LAN" on page 101.)

Important

Both methods leverage multiple BSSID and Virtual LAN (VLAN) technologies that are built-in to the Gateway 7001 Series self-managed AP. The internal and guest networks are implemented as multiple BSSIDs on the same access point, each with different network names (SSIDs) on the Wireless interface and different VLAN IDs on the Wired interface.

On the dual-band radio (Gateway 7001 802.11 A+G Wireless Access Point), the Guest Login settings apply to both Radio One and Radio Two.

Configuring the guest interface

To configure the Guest interface:

1 Do one of the following:

Configure the access point to represent two physically separate networks as described in the following section, see "Configuring a physically separate guest network" on page 100.

OR -

Configure the access point to represent two virtually separate networks as described in the following section, see "Configuring a guest network on a virtual LAN" on page 101.

2 Set up the guest welcome screen for the guest captive portal as described in the following section, see "Configuring the guest welcome screen (captive portal)" on page 101.

Important

Guest Interface settings are not shared among access points across the cluster. These settings must be configured individually on the Administration pages for each access point.

To get to the Administration pages for an access point that is a member of the current cluster, click on its IP Address link on the **Cluster > Access Points** page of the current AP.

For more information about which settings are shared by the cluster and which are not, see "Which settings are shared in the cluster configuration and which are not?" on page 43.

Configuring a physically separate guest network

To configure a physically separate guest network:

1 Make two wired connections from the network ports on the access point: one to your secure, internal LAN and the other to a guest network. (See "Setting up connections for a guest network" on page 19.)

2 Configure Ethernet (Wired) settings for physically separate internal and guest networks on VLANs as described in the sections in "Configuring an Ethernet (wired) interface" on page 68.

(Start by choosing **For Internal and Guest access, use two: Ethernet Ports** as described in "Specifying a physical or virtual Guest network" on page 70.)

3 Provide the radio interface settings and network names (SSIDs) for both internal and guest networks as described in "Configuring a wireless interface" on page 74.

4 Configure other settings on the access point as needed (not necessarily specific to the guest network) as described in this guide.

Configuring a guest network on a virtual LAN

Important

If you want to configure the Guest and Internal networks on Virtual LAN (VLANs), the switch and DHCP server you are using must support VLANs.

As a prerequisite step, configure a port on the switch for handling VLAN tagged packets as described in the IEEE 802.1Q standard.

Guest Welcome Screen settings are shared among access points across the cluster. When you update these settings for one access point, the configuration will be shared with the other access points in the cluster. For more information about which settings are shared by the cluster and which are not, see "Which settings are shared in the cluster configuration and which are not?" on page 43.

To configure internal and guest networks on virtual LANs:

1 Configure Ethernet (Wired) settings for internal and guest networks on VLANs as described in the sections in "Configuring an Ethernet (wired) interface" on page 68.

(Start by choosing **For Internal and Guest access, use two: VLANs** as described in "Specifying a physical or virtual Guest network" on page 70.)

2 Provide the radio interface settings and network names (SSIDs) for both internal and guest networks as described in "Configuring a wireless interface" on page 74.

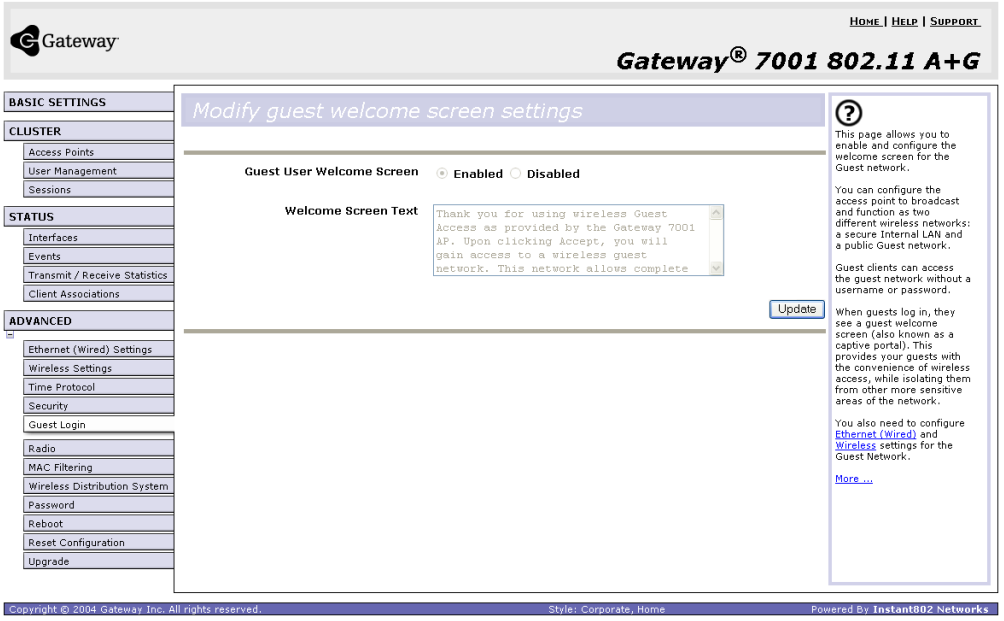
3 Configure other settings on the access point as needed (not necessarily specific to the guest network) as described in this Administration Guide.

Configuring the guest welcome screen (captive portal)

You can set up or modify the welcome screen guest clients see when they open a Web browser or try to browse the Web.

To set up the captive portal:

1 Click **Advanced > Guest Login** on the *Administration* Web page. The *Modify guest welcome screen settings* screen opens.



2 Choose **Enabled** to activate the welcome screen.

3 In the **Welcome Screen Text** box, type the text message you would like guest clients to see on the captive portal.

4 Click **Update** to apply the changes.

Using the guest network as a client

After the guest network is configured, a client can access the guest network.

To access the guest network:

1 A guest client enters an area of coverage and scans for wireless networks.

2 The guest network advertises itself through a guest SSID or some similar name, depending on how the guest SSID is specified in the administration Web pages for the guest interface.

3 The guest client chooses **Guest SSID**.

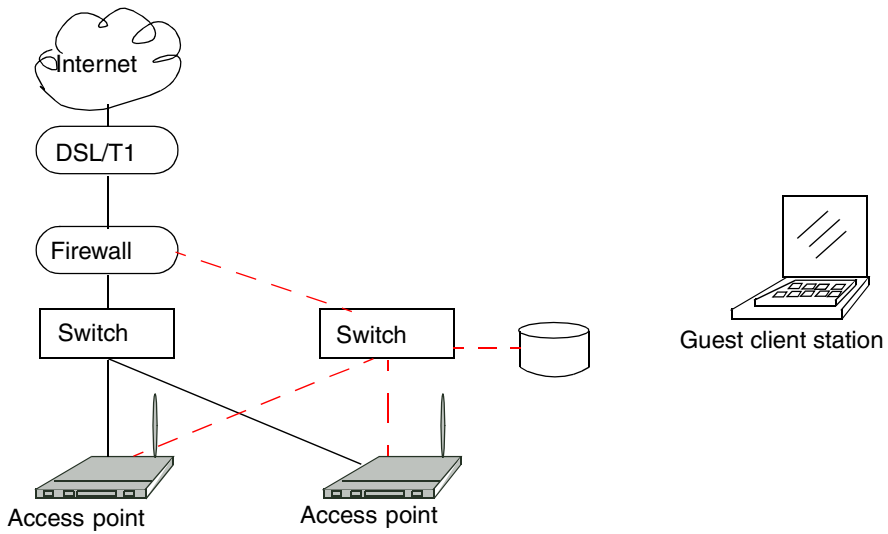
The guest client starts a Web browser and receives a *Guest Welcome* Screen.

The *Guest Welcome* Screen provides a button for the client to click to continue. The guest client can now use the "guest" network.

Deployment example

In the figure, the dotted red lines indicate dedicated guest connections.

All access points and all connections (including guests) are administered from the same Gateway 7001 Series self-managed AP Administration Web pages.



Configuring radio settings

Understanding radio settings

Radio settings directly control the behavior of the radio device in the access point and its interaction with the physical medium, specifically how and what type of electromagnetic waves the AP emits. You can specify whether the radio is on or off, radio frequency (RF) broadcast channel, beacon interval (amount of time between AP beacon transmissions), transmit power, IEEE 802.11 mode in which the radio operates, and so on.

The Gateway 7001 AP is available as a single-band access point (Gateway 7001 802.11G Wireless Access Point), or a dual-band access point (Gateway 7001 802.11A+G Wireless Access Point).

The single band access point can broadcast in either IEEE 802.11b or IEEE 802.11g mode.

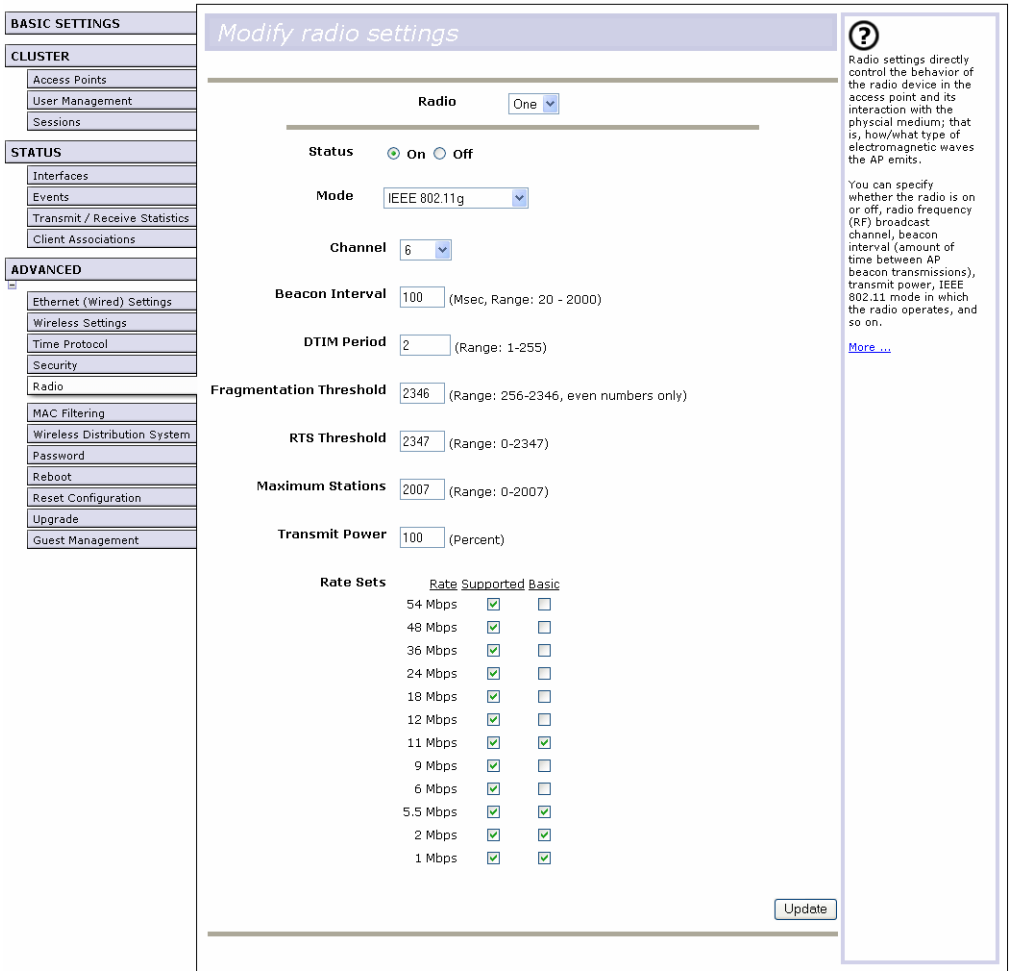
The dual band access point is capable of broadcasting in two different IEEE 802.11 modes simultaneously.

- Radio One can broadcast in IEEE 802.11b or IEEE 802.11g mode.
- Radio Two can broadcast in IEEE 802.11a or IEEE 802.11a Turbo mode.

The IEEE mode along with other radio settings are configured as described in "Navigating to radio settings" on page 105 and "Configuring radio settings" on page 106.

Navigating to radio settings

To specify radio settings, click **Advanced > Radio** on the Administration Web page. The *Modify radio settings* screen opens. Update the boxes as described in the following section.



Configuring radio settings

Field	Description
Radio	The Gateway 7001 Series self-managed AP is available in a dual band and single band version. **Single-Band AP**: If you have the single band version of the Gateway 7001 AP, this box is not included on the Radio tab. **Dual-Band AP**: The dual band access point capable of broadcasting in two different IEEE 802.11 modes simultaneously. • Radio One runs in IEEE 802.11b and IEEE 802.11g modes. • Radio Two runs in IEEE 802.11a and IEEE 802.11a Turbo modes. Specify Radio One or Radio Two. For the dual band AP, the rest of the settings on this tab apply to the radio selected in this box.
Status (On/Off)	Specify whether you want the radio on or off by clicking On or Off.
Mode	The *Mode* defines the Physical Layer (PHY) standard being used by the radio. **Single-Band AP**: For the Single-Band AP, select one of these modes: • IEEE 802.11b • IEEE 802.11g **Dual-Band AP**: For the dual band access point, different modes are available depending on whether you chose Radio One or Radio Two in the Radio box above. For Radio One configuration, select either of these modes: • IEEE 802.11b • IEEE 802.11g For Radio Two configuration, select either of these modes: • IEEE 802.11a • Atheros Turbo 5 GHz (IEEE 802.11a Turbo).
Channel	The *Channel* defines the portion of the radio spectrum that the radio uses for transmitting and receiving. The range of channels and the default channel are determined by the Mode of the radio interface. The Mode can only be set to allow channels within those allowed by the regulatory agencies in the regions for which this device was intended. For most Modes, the default is “Auto”. Auto is the recommended mode because it automatically detects the best channel choices based on signal strength, traffic loads, and so on.

Field	Description
Beacon Interval	*Beacon* frames are transmitted by an access point at regular intervals to announce the existence of the wireless network. The default behavior is to send a beacon frame once every 100 milliseconds (or 10 per second). The Beacon Interval value is set in milliseconds. Type a value from 20 to 2000.
DTIM Period	The *Delivery Traffic Information Map* (DTIM) message is an element included in some Beacon frames. It indicates which client stations, currently sleeping in low-power mode, have data buffered on the access point awaiting pick-up. The DTIM period you specify here indicates how often the clients served by this access point should check for buffered data still on the AP awaiting pickup. The measurement is in beacons. For example, if you set this to “1” clients will check for buffered data on the AP at every beacon. If you set this to “2”, clients will check on every other beacon. If you set this to 10, clients will check on every 10th beacon.
Fragmentation Threshold	Specify a number between 256 and 2,346 to set the frame size threshold in bytes. The *fragmentation threshold* is a way of limiting the size of packets (frames) transmitted over the network. If a packet exceeds the fragmentation threshold set here, the fragmentation function will be activated and the packet will be sent as multiple 802.11 frames. If the packet being transmitted is equal to or less than the threshold, fragmentation will not be used. Setting the threshold to the largest value (2,346 bytes) effectively disables fragmentation. Fragmentation involves more overhead both because of the extra work of dividing up and reassembling of frames it requires, and because it increases message traffic on the network. However, fragmentation can help improve network performance and reliability if correctly configured. Sending smaller frames (by using lower fragmentation threshold) may help with some interference problems, such as with microwave ovens. By default, fragmentation is off. We recommend not using fragmentation unless you suspect radio interference. The additional headers applied to each fragment increase the overhead on the network and can greatly reduce throughput.

Field	Description
RTS Threshold	Specify an RTS Threshold value between 0 and 2347. The RTS threshold specifies the packet size of a request to send (RTS) transmission. This helps control traffic flow through the access point, especially one with a lot of clients. If you specify a low threshold value, RTS packets will be sent more frequently. This will consume more bandwidth and reduce the throughput of the packet. On the other hand, sending more RTS packets can help the network recover from interference or collisions which might occur on a busy network, or on a network experiencing electromagnetic interference.
Maximum Stations	Specify the maximum number of stations allowed to access this access point at any one time. You can type a value between 0 and 2007.
Transmit Power	Provide a percentage value to set the transmit power for this access point. The default is to have the access point transmit using 100 percent of its power. Power settings can only be varied within the settings allowed by the regulatory certifications of the region for which this device was intended. **Recommendations:** • For most cases, we recommend keeping the default and having the transmit power set to 100 percent. This is more cost-efficient as it gives the access point a maximum broadcast range, and reduces the number of APs needed. • To increase capacity of the network, place APs closer together and reduce the value of the transmit power. This will help reduce overlap and interference among APs. A lower transmit power setting can also keep your network more secure because weaker wireless signals are less likely to propagate outside of the physical location of your network.
Rate Sets	Check the transmission rate sets you want the access point to support and the basic rate sets you want the access point to advertise. Rates are expressed in megabits per second. • *Supported Rate Sets* indicate rates that the access point supports. You can check multiple rates (click a checkbox to select or de-select a rate). The AP will automatically choose the most efficient rate based on factors like error rates and distance of client stations from the AP. • *Basic Rate Sets* indicate rates that the access point will advertise to the network for the purposes of setting up communication with other APs and client stations on the network. It is generally more efficient to have an AP broadcast a subset of its supported rate sets.

Updating settings

To apply your changes, click **Update**.

Important

If you are using the dual band version of the Gateway 7001 Series self-managed AP, keep in mind that both Radio One and Radio Two are configured on this tab. The displayed settings apply to either Radio One or Radio Two, depending on which radio you choose in the Radio box (the first box on the tab).

When you have configured settings for one of the radios, click **Update,** then select and configure the other radio. Make sure to click **Update** to apply the second set of configuration settings for the other radio.

Controlling access by MAC address filtering

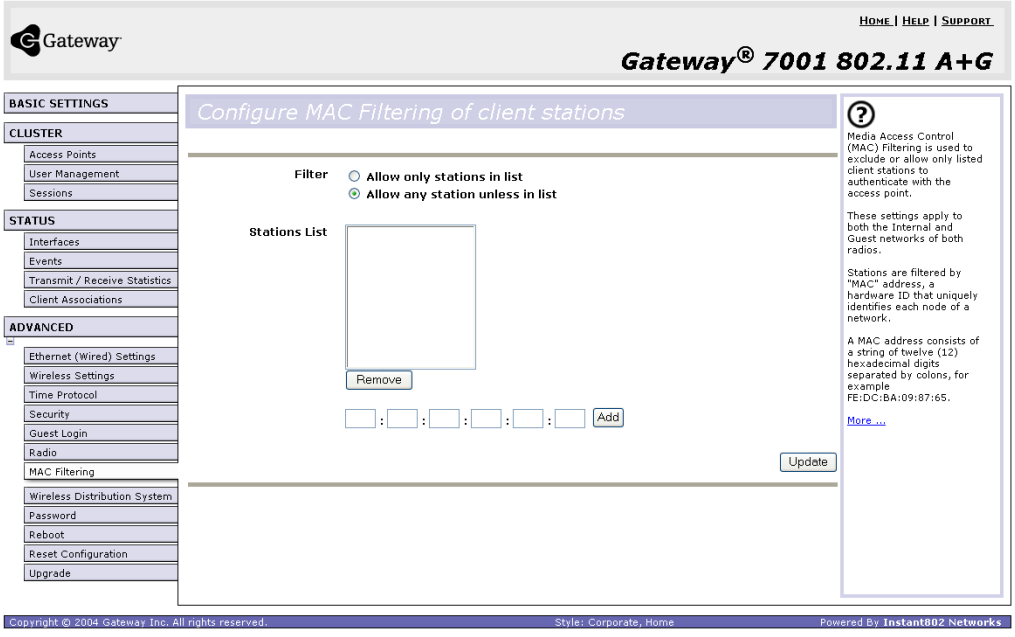
A *Media Access Control* (MAC) address is a hardware address that uniquely identifies each node of a network. All IEEE 802 network devices share a common 48-bit MAC address format, usually displayed as a string of 12 hexadecimal digits separated by colons, for example FE:DC:BA:09:87:65.

Each wireless network interface card (NIC) used by a wireless client has a unique MAC address.

You can control client access to your wireless network by switching on MAC filtering and specifying a list of approved MAC addresses. When MAC filtering is on, only clients with a listed MAC address can access the network.

Navigating to MAC filtering settings

To enable filtering by MAC address, click **Advanced > MAC Filtering** on the *Administration* Web page. The *Configure MAC filtering of client stations* screen opens. Update the boxes as described in the following section.



Using MAC address filtering

This page lets you control access to Gateway 7001 Series self-managed AP based on Media Access Control (MAC) addresses. Based on how you set the filter, you can allow only client stations with a listed MAC address or prevent access to the stations listed.

For the guest interface, MAC filtering settings apply to both BSSes.

Field	Description
Filter	To set the MAC Address Filter, click one of the following options: • Allow only stations in the list • Allow any station unless in list
Stations List	To add a MAC Address to Stations List, type its 48-bit MAC address into the lower text boxes, then click **Add**. The MAC Address is added to the Stations List. To remove a MAC Address from the Stations List, select its 48-bit MAC address, then click **Remove**. The stations in the list will either be allowed or prevented from accessing the AP based on how you set the filter.

Updating settings

To apply your changes, click **Update**.

Configuring a Wireless Distribution System (WDS)

The Gateway 7001 Series self-managed AP lets you connect multiple access points using a Wireless Distribution System (WDS). WDS lets access points communicate with one another wirelessly in a standardized way. This capability is critical in providing a seamless experience for roaming clients and for managing multiple wireless networks. It can also simplify the network infrastructure by reducing the amount of cabling required.

Understanding the WDS

A *Wireless Distribution System* (WDS) is an 802.11f technology that wirelessly connects access points, known as Basic Service Sets (BSS), to form what is known as an Extended Service Set (ESS).

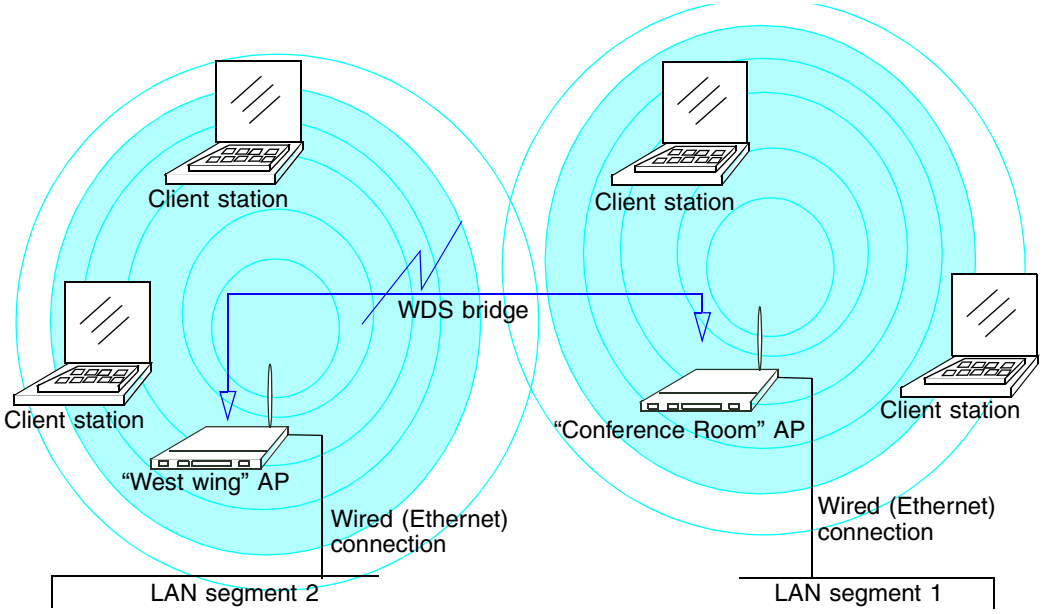
Important

A BSS generally equates to an access point (deployed as a single-AP wireless "network"), except in cases where multi-BSSID features make a single access point look like two or more access points to the network. In such cases, the access point has multiple unique BSSIDs.

Using WDS to bridge distant wired LANs

In an ESS, a network of multiple access points, each access point serves part of an area which is too large for a single access point to cover. You can use WDS to bridge distant Ethernets to create a single LAN. For example, suppose you have one access point which is connected to the network by Ethernet and serving multiple client stations in the

Conference Room (LAN 1), and another Ethernet-wired access point serving stations in the West Wing offices (LAN 2). You can bridge the Conference Room and West Wing access points with a WDS link to create a single network for clients in both areas.

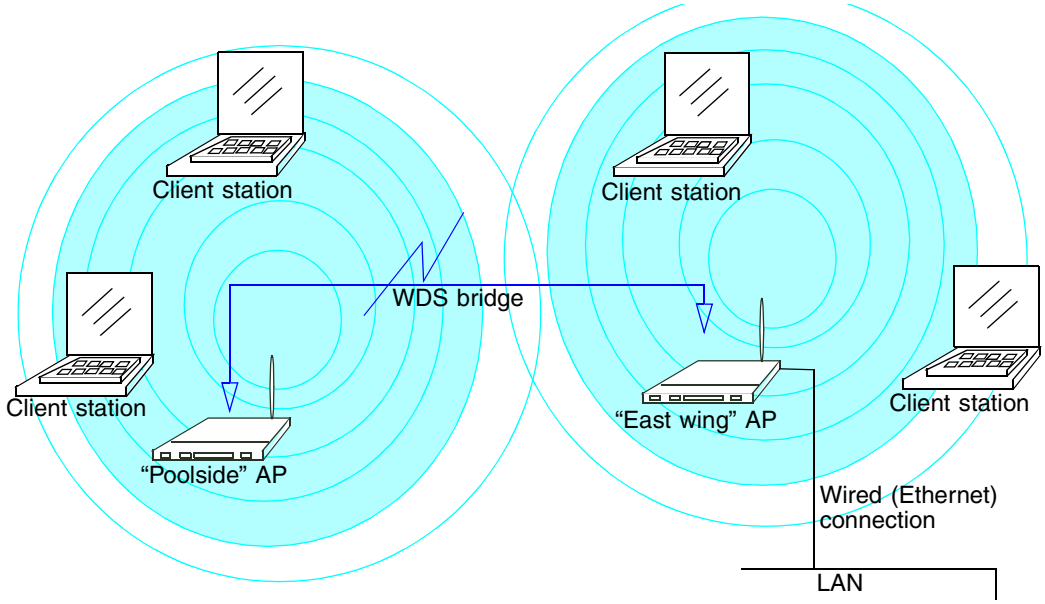


Using WDS to extend the network beyond the wired coverage area

An ESS can extend the reach the network into areas where cabling would be difficult, costly, or inefficient.

For example, suppose you have an access point which is connected to the network by Ethernet and serving multiple client stations in one area ("East Wing - LAN 1" in our example) but cannot reach others which are out of range. Suppose also that it is too difficult or too costly to wire the distant area with Ethernet cabling. You can solve this problem

by placing a second access point closer to second group of stations (“Poolside” in our example) and bridge the two APs with a WDS link. This *extends* your network wirelessly by providing an extra hop to get to distant stations.



Backup links and unwanted loops in WDS bridges

Another use for WDS bridging, the creation of backup links, is not supported in this release of the Gateway 7001 Series self-managed AP. The topic is included here to emphasize that you should not try to use WDS in this way. Backup links will result in unwanted, endless loops of data traffic

If an access point provides *Spanning Tree Protocol* (STP), WDS can be used to configure backup paths between access points across the network. For example, between two access points you could have both a primary path through Ethernet and a secondary (backup) wireless path through a WDS link. If the Ethernet connection goes down, STP would reconfigure its map of the network and effectively fix the down network segment by activating the backup wireless path.

The Gateway 7001 Series self-managed AP does not provide STP for this release. Without STP, it is possible that both connections (paths) may be active at the same time, and result in an endless loop of traffic on the LAN.

Therefore, be sure not create loops with either WDS bridges or combinations of Wired (Ethernet) connections and WDS bridges.

For more information, see the “Do not create loops” note under “Configuring WDS settings” on page 117.

Security considerations related to WDS bridges

Static *Wired Equivalent Privacy* (WEP) is a data encryption protocol for 802.11 wireless networks. Both access points in a given WDS link must be configured with the same security settings. For static WEP, either a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared Key is specified for data encryption.

You can enable Static WEP on the WDS link (bridge). When WEP is enabled, all data exchanged between the two access points in a WDS link is encrypted using a fixed WEP key that you provide.

Static WEP is the only security mode available for the WDS link, and it does not provide effective data protection to the level of other security modes available for service to client stations. If you use WDS on a LAN intended for secure wireless traffic you are putting your network at risk. Therefore, we recommend using WDS to bridge the guest network only for this release. Do not use WDS to bridge access points on the internal network unless you are not concerned about the security risk for data traffic on that network.

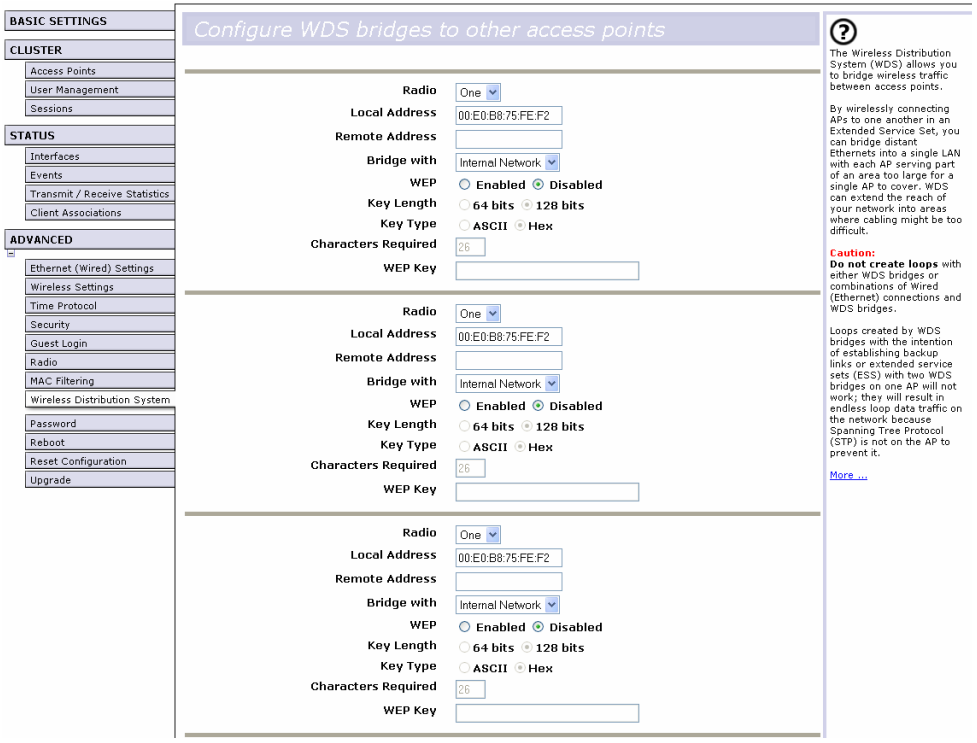
For more information about the effectiveness of different security modes, see "Configuring network security" on page 80. This topic also covers use of plain text security mode for AP-to-station traffic on the guest network, which is intended for less sensitive data traffic.

Navigating to WDS settings

To specify the details of traffic exchange from this access point to others, click **Advanced > Wireless Distribution System** on the Administration Web page. The *Configure WDS bridges to other access points* screen opens. Update the boxes as described in the following section.

Important

The following figure shows the WDS settings page for the dual band AP (Gateway 7001 802.11 A+G Wireless Access Point). The Administration Web page for the single band AP (Gateway 7001 802.11 G Wireless Access Point) will look slightly different.



Configuring WDS settings

The following notes summarize some critical guidelines regarding WDS configuration. Read all the notes before proceeding with WDS configuration.

Important

- The only security mode available on the WDS link is Static WEP, which is not particularly secure. Therefore, we recommend using WDS to bridge the guest network only for this release.

  Do not use WDS to bridge access points on the internal network unless you are not concerned about the security risk for data traffic on that network.

- When using WDS, be sure to configure WDS settings on both access points participating in the WDS link.

- You can have only one WDS link between any pair of access points. That is, a remote MAC address may appear only once on the WDS page for a particular access point.

- Both access points participating in a WDS link must be on the same Radio channel and using the same IEEE 802.11 mode. (See “Configuring radio settings” on page 104 for information on configuring the Radio mode and channel.)

- Do not create loops with either WDS bridges or combinations of Wired (Ethernet) connections and WDS bridges. Spanning Tree Protocol (STP), which manages path redundancy and prevent unwanted loops, is not enabled for this release. Keep these rules in mind when working with WDS on this release of the Gateway 7001 Series self-managed AP:

  Any two access points can be connected by only a single path - either a WDS bridge (wireless) or an Ethernet connection (wired), but not both.

  Do not create “backup” links.

  If you can trace more than one path between any pair of APs going through any combination of Ethernet or WDS links, you have a loop.

  You can only extend or bridge either the internal or guest network but not both.

To configure WDS on this access point, describe each AP intended to receive hand-offs and send information to this AP. Each destination AP needs the following description.

Field	Description
Radio	The Gateway 7001 AP is available in a dual band and single band version. **Single-Band AP**: On the single band version of the Gateway® 7001 AP, this box is not included on the WDS tab. **Dual-Band AP**: For each WDS link on a dual-band AP, select Radio One or Radio Two. The rest of the settings for the link apply to the radio selected in this box. The read-only "Local Address" will change depending on which Radio you select here.
Local Address	Indicates the Media Access Control (MAC) addresses for this access point. A MAC address is a permanent, unique hardware address for any device that represents an interface to the network. The MAC address is assigned by the manufacturer. You cannot change the MAC address. It is provided here for informational purposes as a unique identifier for the access point or interface. **Single-Band AP**: On the single band version of the Gateway® 7001 AP, a single MAC address is shown at the top of the WDS settings page. The address shown for the single-band radio is the MAC address for the bridge (br0). This is the address by which the AP is known externally to other networks. **Dual-Band AP**: For each WDS link on a dual-band AP, the Local Address reflects the MAC address for the internal interface on the selected radio (Radio One on WLAN0 or Radio Two WLAN1).
Remote Address	Specify the MAC address of the destination access point, that is, the access point to which data will be sent or "handed-off" and from which data will be received.
Bridge with	The Gateway 7001 Series self-managed AP provides the capability of setting up guest and internal networks on the same access point. (See "Setting up Guest Access" on page 99.) The guest network typically provides internet access but isolates guest clients from more sensitive areas of your internal network. It is common to have security disabled on the guest network to provide open access. Alternatively, the internal network provides full access to protected information behind a firewall and requires secure logins or certificates for access. When using WDS to link up one access point to another, you need to identify within which of these networks you want the data exchange to occur. Specify the network to which you want to bridge this access point: • Internal Network • Guest Network

Field	Description
WEP	Specify whether you want Wired Equivalent Privacy (WEP) encryption enabled for the WDS link. • Enabled • Disabled *Wired Equivalent Privacy* (WEP) is a data encryption protocol for 802.11 wireless networks. Both access points on the WDS link must be configured with the same security settings. For static WEP, a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared Key for data encryption.
Key Length	If WEP is enabled, specify the length of the WEP key: • 64 bits • 128 bits
Key Type	If WEP is enabled, specify the WEP key type: • ASCII • Hex
Characters Required	Indicates the number of characters required in the WEP key. The number of characters required updates automatically based on how you set Key Length and Key Type.
WEP Key	Type a string of characters. If you selected “ASCII”, type any combination of 0-9. If you selected “HEX”, type hexadecimal digits (any combination of 0-9 and a-f or A-F). These are the RC4 encryption keys shared with the stations using the access point.

Example of configuring a WDS link

When using WDS, be sure to configure WDS settings on both access points on the WDS link.

To create a WDS link between a pair of access points:

1. Open the Administration Web pages for MyAP1 (for example), by typing the IP address for MyAP1 as a URL in the Web browser address bar in the following form:

   http://IPAddressOfAccessPoint

   where IPAddressOfAccessPoint is the address of MyAP1.

2. Click **WDS** on MyAP1 Administration Web pages.

   The MAC address for MyAP1 (the access point you are currently viewing) will show as the “Local Address” at the top of the page.

3 Configure a WDS interface for data exchange with MyAP2 (for example).

Start by typing the MAC address for MyAP2 as the "Remote Address" and fill in the rest of the boxes to specify the network (guest or internal), security, and so on. Save the settings (click **Update**).

4 Click **Advanced—>Radio** on the Administration Web page to verify or set the mode and the radio channel on which you want MyAP1 to broadcast.

Remember that the two access points participating in the link, MyAP1 and MyAP2, must be set to the same Mode and be transmitting on the same channel.

For our example, let us say we are using IEEE 802.11b Mode and broadcasting on Channel 6. (We would choose Mode and Channel from the lists on the *Radio* screen.)

5 Now repeat the same steps for MyAP2:

- Open Administration Web pages for MyAP2 by using MyAP2's IP address in a URL.
- Click **WDS** on the MyAP2 Administration Web page. (MyAP2's MAC address will show as the "Local Address".)
- Configure a WDS interface for data exchange with MyAP1, starting with the MAC address for MyAP1.
- Navigate to the radio settings for MyAP2 to verify that it is using the same mode and broadcasting on the same channel as MyAP1. (For our example, the Mode is 802.11b and the channel is 6.)
- Be sure to save the settings by clicking **Update**.

Updating settings

To apply your changes, click **Update**.

Configuring security settings on wireless clients

Typically, users will configure security on their wireless clients for access to many different networks (access points). The list of "Available Networks" will change depending on the location of the client and which APs are online and detectable in that location. The exception to this is if the access point is set to prohibit the broadcast of its network name. In this case the SSID will not show up in the list of Available Networks on the client. Instead, the client must have the exact network name configured in the network connection properties before it will be able to connect.

Once an AP has been detected by the client and security is configured for it, it remains in the client's list of networks but shows as either reachable or unreachable depending on the situation. For each network (AP) you want to connect to, configure security settings on the client to match the security mode being used by that network.

We describe security setup on a client that uses Microsoft Windows client software for wireless connectivity. The Windows client software is used as the example because of its widespread availability on Windows computers and laptops. These procedures will vary slightly if you use different software on the client (such as Funk Odyssey), but the configuration information you need to provide is the same.

Important

The recommended sequence for security configuration is (1) set up security on the access point, and (2) configure security on each of the wireless clients.

We expect that initially, you will connect to an access point that has no security set (plain text mode) from an unsecure wireless client. With this initial connection, you can go to the access point Administration Web pages and configure a security mode (**Advanced > Security**).

When you re-configure the access point with a security setting and click **Update**, your wireless client will be disassociated and you will lose connectivity to the AP Administration Web pages. In some cases, you may need to make additional changes to the AP security settings before configuring the client. Therefore, you must have a backup Ethernet (wired) connection.

The following sections describe how to set up each of the supported security modes on wireless clients of a network served by the Gateway 7001 AP.

- "Network infrastructure and choosing between built-in or external authentication server" on page 122
- "Make sure the wireless client software is up-to-date" on page 123
- "Accessing the Microsoft Windows wireless client security settings" on page 123

Network infrastructure and choosing between built-in or external authentication server

Network security configurations including *Public Key Infrastructures* (PKI), *Remote Authentication Dial-in User Server* (RADIUS) servers, and *Certificate Authority* (CA) can vary a great deal from one organization to the next in terms of how they provide *Authentication, Authorization,* and *Accounting* (AAA). Ultimately, the particulars of your infrastructure will determine how clients should configure security to access the wireless network. Rather than try to predict and address the details of every possible scenario, this document provides general guidelines about each type of client configuration supported by the Gateway 7001 AP.

I want to use the built-in authentication server (EAP-PEAP)

If you do not have a RADIUS server or PKI infrastructure in place or if you are unfamiliar with many of these concepts, we strongly recommend setting up the Gateway 7001 APs with security that uses the built-in authentication server on the AP. This will mean setting up the AP to use either IEEE 802.1x or WPA with RADIUS security mode. (The built-in authentication server uses EAP-PEAP authentication protocol.)

- If the Gateway 7001 AP is set up to use IEEE 802.1x mode and the Built-in Authentication Server, then configure wireless clients as described in "IEEE 802.1x client using EAP/PEAP" on page 129.
- If the Gateway 7001 AP is configured to use WPA with RADIUS mode and the Built-in Authentication Server, configure wireless clients as described in "WPA with RADIUS client using EAP/PEAP" on page 137.

I want to use an external RADIUS server with EAP-TLS certificates or EAP-PEAP

We make the assumption that if you have an external RADIUS server and PKI/CA setup, you will know how to configure client security options appropriate to your security infrastructure beyond the fundamental suggestions given here. Topics covered here that particularly relate to client security configuration in a RADIUS - PKI environment are:

- "IEEE 802.1x client using EAP-TLS certificate" on page 133
- "WPA with RADIUS client using EAP-TLS certificate" on page 141
- "Configuring an external RADIUS server to recognize the Gateway 7001 AP" on page 146
- "Obtaining a TLS-EAP certificate for a client" on page 151

Details on how to configure an EAP-PEAP client with an external RADIUS server are not covered in this document.

Make sure the wireless client software is up-to-date

Before setting up the client systems, keep in mind that service packs, patches, and new releases of drivers as well as other supporting technologies for wireless clients are being generated at a fast pace. A common problem encountered in client security setup is that the latest driver for the wireless interface or patches required for the operating system to properly function with the security type being configured is not installed. For example, if you are setting up WPA on the client, make sure you have a driver installed that supports WPA as well as any operating system updates relating to WPA to support the relatively new technology. Also keep in mind, many wireless client cards currently available do not ship from the factory with the latest drivers.

Accessing the Microsoft Windows wireless client security settings

Generally, on Microsoft Windows XP there are two ways to get to the security properties for a wireless client:

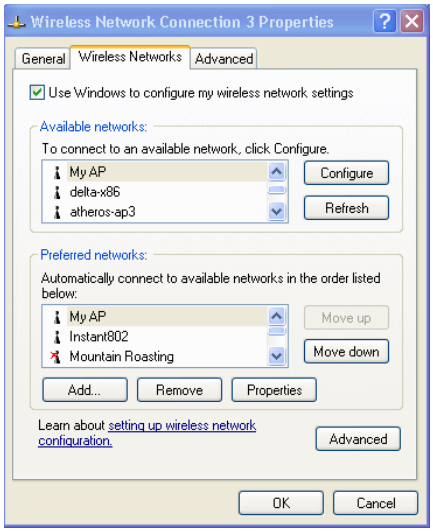
To access the security properties for a wireless client:

1. From the wireless connection icon on the Windows task bar:
   a. Right-click the wireless connection icon in your Windows task bar and select **View available wireless networks**.
   b. Select the SSID of the network to which you want to connect and click **Advanced** to open the Wireless Network Connection Properties dialog.

OR -

1. From the Windows **Start** menu at the left end of the task bar:
   a. Choose **Start > My Network Places** to open the *Network Connections* window.
   b. From the **Network Tasks** menu on the left, click **View Network Connections** to open the *Network Connections* window.
   c. Right-click the wireless network connection you want to configure, then choose **View available wireless networks**.

d Select the SSID of the network to which you want to connect, then click **Advanced.** The *Wireless Network Connection Properties* dialog box, which lists available networks and preferred networks, opens.

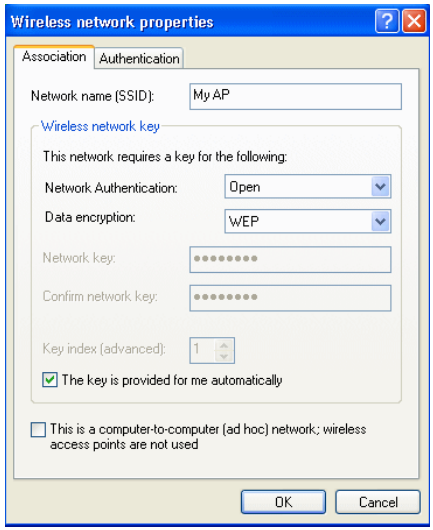


The list of available networks will change depending on client location. Each network (or access point) that is detected by the client shows up in this list. ("Refresh" updates the list with current information.)

For each network you want to connect to, configure security settings on the client to match the security mode being used by that network.

Note: If the AP is configured to prohibit broadcast of its network name, the name will not show on this list. In that case you would need to type in the exact network name to be able to connect to it.

2 From the list of Available networks select the SSID of the network to which you want to connect, then click Configure. The *Wireless Network Connection Properties* dialog box opens (with the Association and Authentication tabs for the selected network).



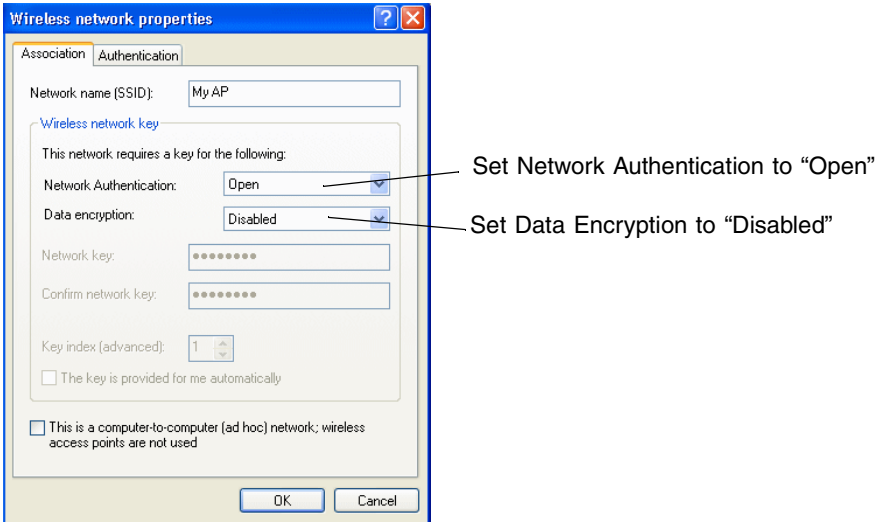
Use this dialog box for configuring all the different types of client security described in the following sections. Make sure that the *Wireless Network Properties* dialog box you are working in pertains to the Network Name (SSID) for the network you want to reach on the wireless client you are configuring.

Configuring a client to access an unsecure network (plain text mode)

If the access point or wireless network to which you want to connect is configured as "Plain Text" security mode (no security), you need to configure the client accordingly. A client using no security to connect is configured with Network Authentication "Open" to that network and Data Encryption "Disabled" as described below.

If you do have security configured on a client for properties of an unsecure network, the security settings actually can prevent successful access to the network because of the mismatch between client and access point security configurations.

To configure the client to not use any security, open the client *Network Properties* dialog box and configure the following settings.

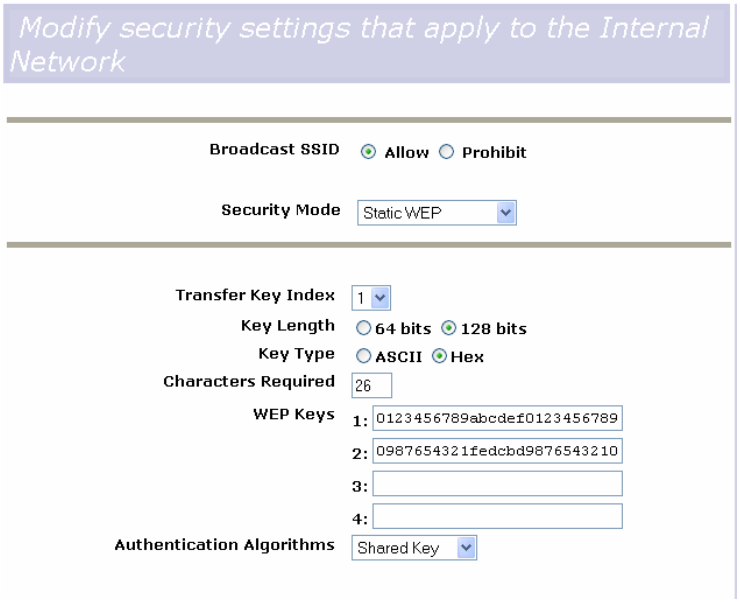


Association Tab	Network Authentication	Open
	Data Encryption	Disabled

Configuring static WEP security on a client

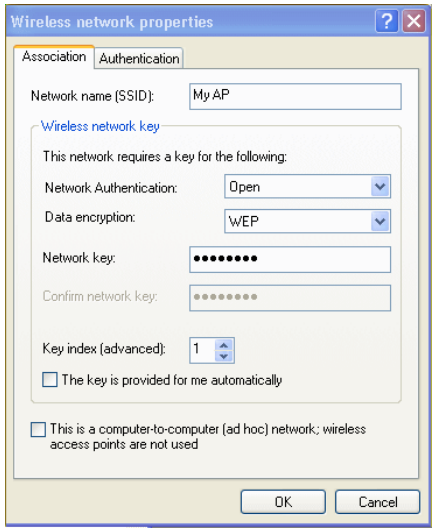
Static *Wired Equivalent Privacy* (WEP) encrypts data moving across a wireless network based on a static (non-changing) key. The encryption algorithm is a “stream” cipher called RC4. The access point uses a key to transmit data to the client stations. Each client must use that same key to decrypt data it receives from the access point. Different clients can use different keys to transmit data to the access point. (Or they can all use the same key, but this is less secure because it means one station can decrypt the data being sent by another.)

If you configured the Gateway 7001 AP to use Static WEP security mode, as shown in the following illustration, you need to configure WEP security on each client.



To configure WEP security on each client:

1. On the *Network Properties* dialog box, select the **Association** tab. The *Association* dialog box opens.



2. Select **Open** or **Shared** in the Network Authentication list, then select **WEP** in the Data encryption list.

3. Type a Network key in the box provided.

   Make sure the network key matches the WEP key on the access point in the position selected to the **Key index (advanced)**.

   Retype to confirm.

4. As an option you can select a different transfer key index (in the Key index list) to send data from the client back to the access point.

5. Click to clear the **The key is provided for me automatically** check box.

6. Click **OK** to save your settings and close.

Association Tab	Network Authentication	**Open** or **Shared**, depending on how you configured this option on the access point. **Note:** When the Authentication Algorithm on the access point is set to **Both**, clients set to either Shared or Open can associate with the AP. Clients configured to use WEP in Shared mode must have a valid WEP key in order to associate with the AP. Clients configured to use WEP as an Open system can associate with the AP even without a valid WEP key (but a valid key will be required to actually view and exchange data). For more information, see Administrators Guide and Online Help on the access point.
	Data Encryption	WEP
	Network Key	Provide the WEP key you entered on the access point Security settings in the Transfer Key Index position. For example, if the Transfer Key Index on the access point is set to **1**, then for the client Network Key specify the WEP Key you entered as WEP Key 1 on the access point.
	Key Index	Set key index to indicate which of the WEP keys specified on the access point Security page will be used to transfer data from the client back to the access point. For example, you can set this to **1**, **2**, **3**, or **4** if you have all four WEP keys configured on the access point.
	The key is provided for me automatically	Disable this option (click to clear the check box).
	Enable IEEE 802.1x authentication for this network	Make sure that IEEE 802.1x authentication is disabled (box should be unchecked). (Setting the encryption mode to WEP should automatically disable authentication.)

Connecting to the wireless network with a static WEP client

Static WEP clients should now be able to associate and authenticate with the access point. As a client, you will not be prompted for a WEP key. The WEP key configured on the client security settings is automatically used when you connect.

Configuring IEEE 802.1x security on a client

IEEE 802.1x is the standard defining port-based authentication and infrastructure for doing key management. *Extensible Authentication Protocol* (EAP) messages are sent over an IEEE 802.11 wireless network using a protocol called EAP Encapsulation Over LANs (EAPOL). IEEE 802.1x provides dynamically-generated keys that are periodically refreshed. An RC4 stream cipher is used to encrypt the frame body and cyclic redundancy checking (CRC) of each 802.11 frame.

IEEE 802.1x client using EAP/PEAP

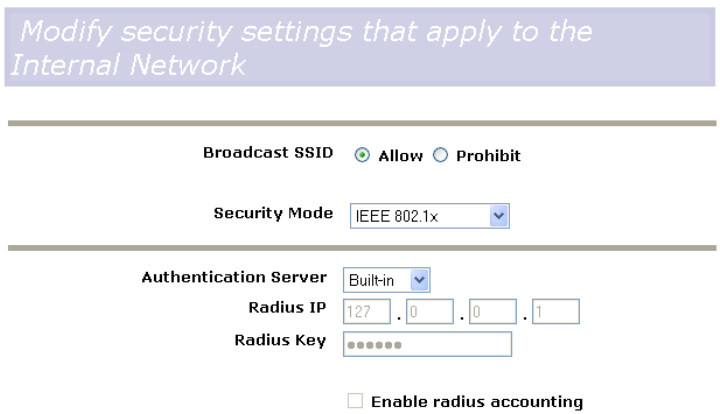
The Built-In Authentication Server on the Gateway 7001 AP uses Protected *Extensible Authentication Protocol* (EAP) referred to here as "EAP/PEAP".

- If you are using the Built-in Authentication server with "IEEE 802.1x" security mode on the Gateway 7001 AP, then you will need to set up wireless clients to use PEAP.
- Additionally, you may have an external RADIUS server that uses EAP/PEAP. If so, you will need to (1) add the Gateway 7001 AP to the list of RADIUS server clients, and (2) configure your IEEE 802.1x wireless clients to use PEAP.

Important

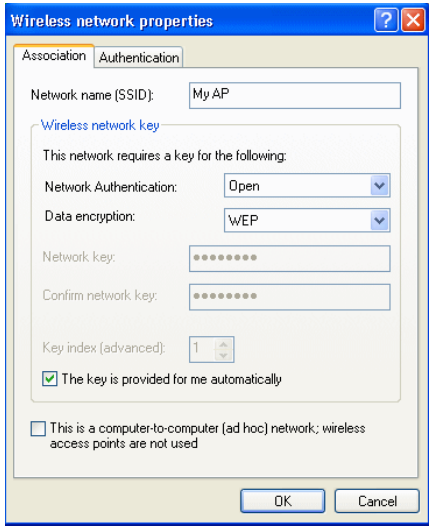
The following example assumes you are using the Built-in Authentication server that comes with the Gateway® 7001 AP. If you are setting up EAP/PEAP on a client of an AP that is using an external RADIUS server, the client configuration process will differ somewhat from this example especially with regard to certificate validation.

If you configured the Gateway 7001 AP to use IEEE 802.1x security mode, as shown in the following illustration, you need to configure IEEE 802.1x security with PEAP authentication on each client.



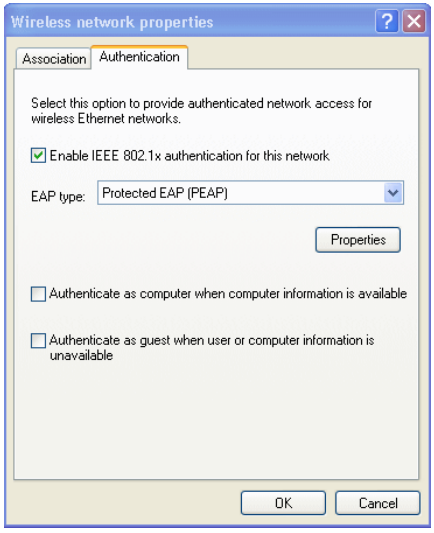
To configure the clients with IEEE 802.1x security with PEAP authentication:

1 On the *Network Properties* dialog box, select the **Association** tab. The *Association* dialog box opens.

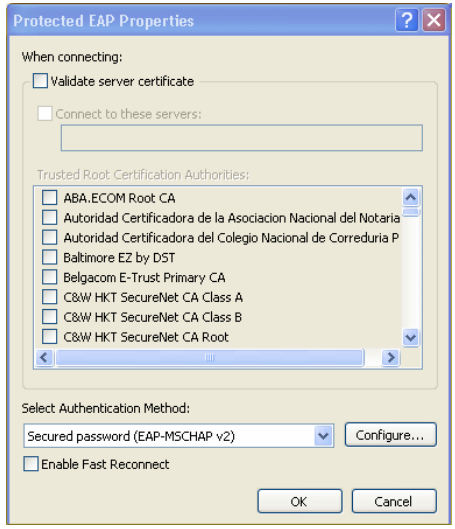


2 Select **Open** in the Network Authentication list, select **WEP** in the Data Encryption list, then click to select the **The key is provided for me automatically** check box.

3 Click the **Authentication** tab. The *Authentication* dialog box opens.



4 Click to select the **Enable IEEE 802.1x authentication for this network** check box, select **Protected EAP (PEAP)** from the EAP type list, then click **Properties**. The *Protected EAP Properties* dialog box opens.



5 Click to clear the **Validate server certificate** check box, select **Secured password (EAP-MSCHAP v2)** from the Select Authentication Method list, then click **Configure**. The *EAP MSCHAP v2 Properties* dialog box opens.

6 Click to clear the **Automatically use my Windows login name and password (and domain, if any)** check box, then click **OK**.

7 Click **OK** on each dialog box to close and save your changes.

Association Tab	Network Authentication	Open
	Data Encryption	WEP **Note:** An RC4 stream cipher is used to encrypt the frame body and cyclic redundancy checking (CRC) of each IEEE 802.11 frame. This is the same encryption algorithm as is used for Static WEP; therefore, the data encryption method configured on the client for this mode is WEP.
	This key is provided for me automatically	Enable (click to check) this option
Authentication Tab	EAP Type	Choose **Protected EAP (PEAP**)
Protected EAP Properties dialog box	Validate Server Certificate	Disable this option (click to clear the check box). **Note:** This example assumes you are using the Built-in Authentication server on the AP. If you are setting up EAP/PEAP on a client of an AP that is using an external RADIUS server, you might certificate validation and choose a certificate, depending on your infrastructure.
	Select Authentication Method	Choose **Secured password (EAP-MSCHAP v2)**

Logging on to the Wireless Network with an IEEE 802.1x PEAP Client

IEEE 802.1x PEAP clients should now be able to associate with the access point. Client users will be prompted for a user name and password to authenticate with the network.

IEEE 802.1x client using EAP-TLS certificate

Extensible Authentication Protocol (EAP) Transport Layer Security (TLS), or EAP-TLS, is an authentication protocol that supports the use of smart cards and certificates. You have the option of using EAP-TLS with both WPA with RADIUS and IEEE 802.1x modes if you have an external RADIUS server on the network to support it.

Important

If you want to use IEEE 802.1x mode with EAP-TLS certificates for authentication and authorization of clients, you must have an external RADIUS server and a Public Key Authority Infrastructure (PKI), including a Certificate Authority (CA), server configured on your network. It is beyond the scope of this document to describe the configuration of the RADIUS server, PKI, and CA server. Consult the documentation for those products.

Some good starting points available on the Web for the Microsoft Windows PKI software are: "How to Install/Uninstall a Public Key Certificate Authority for Windows 2000" at http://sup-port.microsoft.com/default.aspx?scid=kb;EN-US;231881 and "How to Configure a Certificate Server" at http://support.microsoft.com/default.aspx?scid=kb;en-us;318710#3

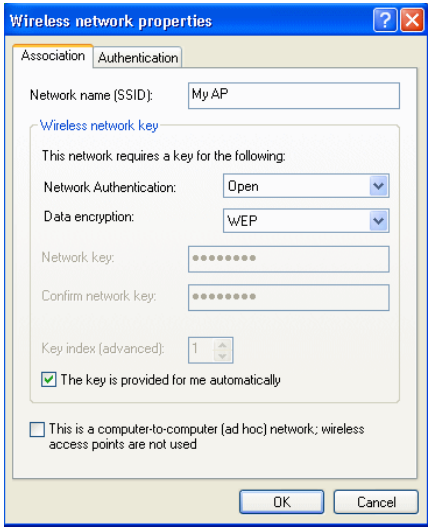
To set up an IEEE 802.1x client using EAP-TLS Certificate security:

1. Add the Gateway 7001 AP to the list of RADIUS server clients. (See "Configuring an external RADIUS server to recognize the Gateway 7001 AP" on page 146.)
2. Configure the Gateway 7001 AP to use your RADIUS server (by providing the RADIUS server IP address as part of the "IEEE 802.1x" security mode settings).
3. Configure wireless clients to use IEEE 802.1x security and "Smart Card or other Certificate" as described in this section.
4. Obtain a certificate for this client as described in "Obtaining a TLS-EAP certificate for a client" on page 151.

If you configured the Gateway 7001 AP to use IEEE 802.1x security mode with an external RADIUS server, you need to configure IEEE 802.1x security with certificate authentication on each client.

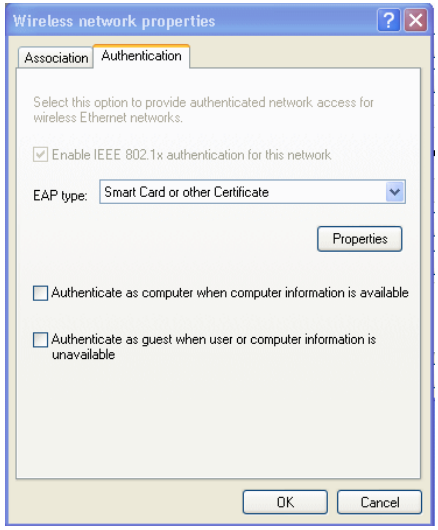
To configure each client for IEEE 802.1x security with certificate authentication:

1. On the *Network Properties* dialog box, select the **Association** tab. The *Association* dialog box opens.

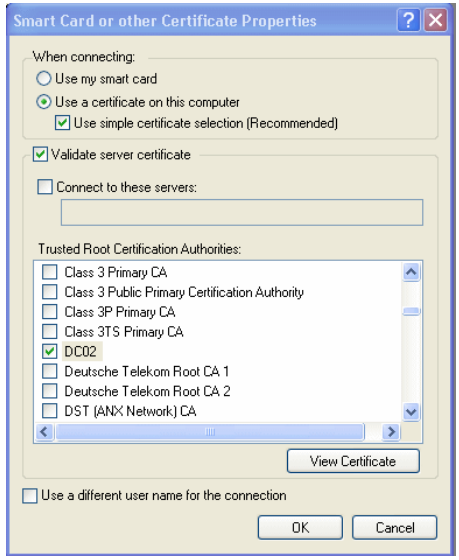


2. Select **Open** in the Network Authentication list, select **WEP** in the Data Encryption list, then click to select the **The key is provided for me automatically** check box.

3 Click the **Authentication** tab. The *Authentication* dialog box opens.



4 Click to select the **Enable IEEE 802.1x authentication for this network** check box, select **Smart Card or other Certificate** from the EAP type list, then click **Properties**. The *Smart Card or other Certificate Properties* dialog box opens.



5 Enable the **Validate server certificate** option, then select the name of the certificate you downloaded for this client in step 4 of the previous procedure. For more information, see "Obtaining a TLS-EAP certificate for a client" on page 151.

6 Click **OK** on each dialog box to close and save the settings.

Association Tab	Network Authentication	Open
	Data Encryption	WEP **Note:** An RC4 stream cipher is used to encrypt the frame body and cyclic redundancy checking (CRC) of each IEEE 802.11 frame. This is the same encryption algorithm as is used for Static WEP; therefore, the data encryption method configured on the client for this mode is WEP.
	This key is provided for me automatically	Enable (click to select) this option
Authentication Tab	Enable IEEE 802.1x authentication for this network	Enable (click to select) this option
	EAP Type	Choose **Smart Card or other Certificate**
Smart Card or other Certificate Properties dialog box	Validate Server Certificate	Enable (click to select) this option.
	Certificates	Select the certificate from the list.

Connecting to the wireless network with an IEEE 802.1x client using a certificate

IEEE 802.1x clients should now be able to connect to the access point using their TLS certificates. The certificate you installed is used when you connect, so you will not be prompted for login information. The certificate is automatically sent to the RADIUS server for authentication and authorization.

Configuring WPA with RADIUS security on a client

Wi-Fi Protected Access (WPA) with Remote Authentication Dial-In User Service (RADIUS) is a Wi-Fi Alliance subset of IEEE 802.11i, which includes Temporal Key Integrity Protocol (TKIP), and Counter mode/CBC-MAC Protocol mechanisms. This mode requires the use of a RADIUS server to authenticate users, and configuration of user accounts on the access point.

When you configure WPA with RADIUS security mode on the access point, you have a choice of whether to use the Built-in Authentication Server or an external RADIUS server that you provide.

The Gateway 7001 AP Built-in Authentication Server supports Protected Extensible Authentication Protocol (EAP) known as "EAP/PEAP" and Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAP V2), which provides authentication for point-to-point (PPP) connections between a Windows-based computer and network devices such as access points.

So, if you configure the network (access point) to use security mode and choose the Built-in Authentication server, you must configure client stations to use WPA with RADIUS and EAP/PEAP.

If you configure the network (access point) to use this security mode with an external RADIUS server, you must configure the client stations to use WPA with RADIUS and whichever security protocol your RADIUS server is configured to use.

WPA with RADIUS client using EAP/PEAP

The Built-In Authentication Server on the Gateway 7001 AP uses Protected Extensible Authentication Protocol (EAP) known as "EAP/PEAP".

- If you are using the Built-in Authentication server with "WPA with RADIUS" security mode on the Gateway 7001 AP, then you will need to set up wireless clients to use PEAP.
- Additionally, you may have an external RADIUS server that uses EAP/PEAP. If so, you will need to (1) configure the RADIUS server and set up user accounts on it, and (2) configure your "WPA with RADIUS" wireless clients to use PEAP.

Important

The following example assumes you are using the Built-in Authentication server that comes with the Gateway 7001 AP. If you are setting up EAP/PEAP on a client of an AP that is using an external RADIUS server, the client configuration process will differ somewhat from this example, especially with regard to certificate validation.

If you configured the Gateway 7001 AP to use WPA with RADIUS security mode and to use either the built-in authentication server or an external RADIUS server that uses EAP/PEAP, you must first set up user accounts on the access point (**Cluster** > **User Management**), then configure WPA security with PEAP authentication on each client.

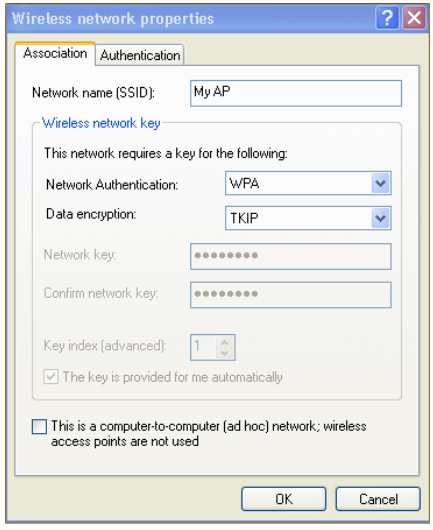
To set up user accounts on the access point:

1 Access the Administration Web page for the access point ("Navigating to basic settings" on page 30), then click **Cluster > User Management**. The *Manage user accounts* screen opens.

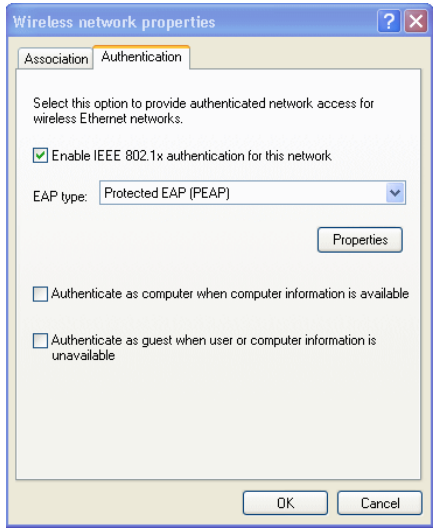
2 Set up user accounts as necessary.

To configure WPA security with PEAP authentication on each client:

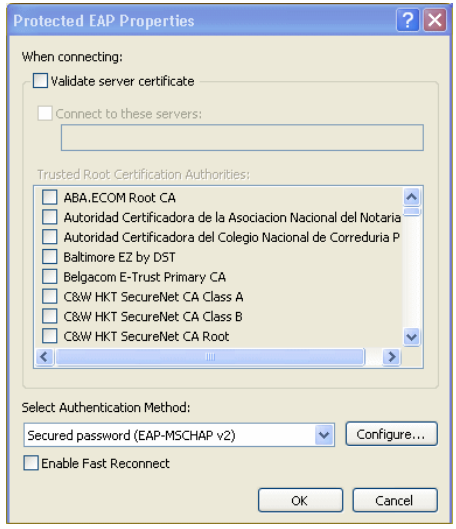
1 On the *Network Properties* dialog box, select the **Association** tab. The *Association* dialog box opens.



2 Select **WPA** in the Network Authentication list, and **TKIP** or **AES** in the Data Encryption list, then click the **Authentication** tab. The *Authentication* dialog box opens.



3 Select **Protected EAP (PEAP)** from the EAP type list, then click **Properties**. The *Protected EAP Properties* dialog box opens.



4 Disable the **Validate server certificate** option, select **Secured password (EAP-MSCHAP v2)** from the Select Authentication Method list, then click **Configure**. The *EAP MSCHAP v2 Properties* dialog box opens.

5 Click (to uncheck) the **Automatically use my Windows login name and password (and domain, if any)** box, then click **OK**.

6 Click **OK** on each dialog box to close and save your changes.

Association Tab	Network Authentication	WPA
	Data Encryption	TKIP or AES, depending on how this option is configured on the access point. **Note:** When the Cipher Suite on the access point is set to **Both**, then TKIP clients with a valid TKIP key and AES clients with a valid CCMP (AES) key can associate with the access point. For more information, see Administrators Guide and Online Help on the access point.
Authentication Tab	EAP Type	Choose **Protected EAP (PEAP)**
Protected EAP Properties dialog box	Validate Server Certificate	Disable this option (click to uncheck the box). This example assumes you are using the Built-in Authentication server on the AP. If you are setting up EAP/PEAP on a client of an AP that is using an external RADIUS server, you might select certificate validation and choose a certificate, depending on your infrastructure.
	Selected Authentication Method	Choose **Secured Password (EAP-MSCHAP v2)**

Logging on to the Wireless Network with a WPA PEAP Client

"WPA with RADIUS" PEAP clients should now be able to associate with the access point. Client users will be prompted for a user name and password to authenticate with the network.

WPA with RADIUS client using EAP-TLS certificate

Extensible Authentication Protocol (EAP) Transport Layer Security (TLS), or EAP-TLS, is an authentication protocol that supports the use of smart cards and certificates. You have the option of using EAP-TLS with both WPA with RADIUS and IEEE 802.1x modes if you have an external RADIUS server on the network to support it.

Important

If you want to use IEEE 802.1x mode with EAP-TLS certificates for authentication and authorization of clients, you must have an external RADIUS server and a Public Key Authority Infrastructure (PKI), including a Certificate Authority (CA), server configured on your network. It is beyond the scope of this document to describe the configuration of the RADIUS server, PKI, and CA server. Consult the documentation for those products.Some good starting points available on the Web for the Microsoft Windows PKI software are: "How to Install/Uninstall a Public Key Certificate Authority for Windows 2000" at http://sup-port.microsoft.com/default.aspx?scid=kb;EN-US;231881 and "How to Configure a Certificate Server" at http://support.microsoft.com/default.aspx?scid=kb;en-us;318710#3.

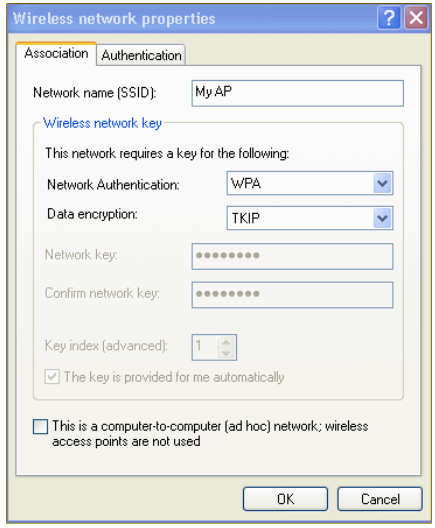
To use this type of security:

1. Add the Gateway 7001 AP to the list of RADIUS server clients. (See "Configuring an external RADIUS server to recognize the Gateway 7001 AP" on page 146.)
2. Configure the Gateway 7001 AP to use your RADIUS server (by providing the RADIUS server IP address as part of the "WPA with RADIUS" security mode settings).
3. Configure wireless clients to use WPA security and "Smart Card or other Certificate" as described in this section.
4. Obtain a certificate for this client as described in "Obtaining a TLS-EAP certificate for a client" on page 151.

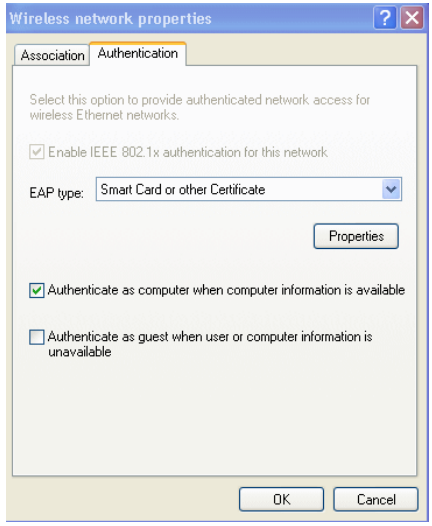
If you configured the Gateway 7001 AP to use WPA with RADIUS security mode with an external RADIUS server, you must configure WPA security with certificate authentication on each client.

To configure WPA security with certificate authentication on each client:

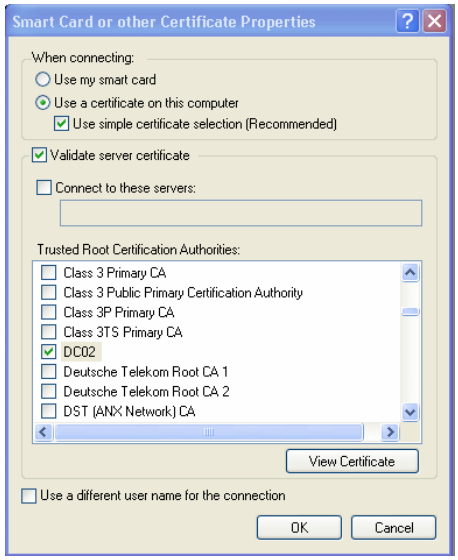
1. On the *Network Properties* dialog box, select the **Association** tab. The *Association* dialog box opens.



2. Select **WPA** in the Network Authentication list, and **TKIP** or **AES** in the Data Encryption list, then click the **Authentication** tab. The *Authentication* dialog box opens.



3 Select **Smart Card or other Certificate** from the EAP Type list, click to select the **Authenticate as computer when computer information is available** check box, then click Properties. The *Smart Card or other Certificate Properties* dialog box opens.



4 Select the **Validate server certificate** option, then select the name of the certificate from the Trusted Root Certification Authorities list. For more information on certificates, see "Obtaining a TLS-EAP certificate for a client" on page 151.

5 Click **OK** on each dialog box to close and save the settings.

Association Tab	Network Authentication	WPA
	Data Encryption	TKIP or AES, depending on how this option is configured on the access point. **Note:** When the Cipher Suite on the access point is set to **Both**, then TKIP clients with a valid TKIP key and AES clients with a valid CCMP (AES) key can associate with the access point. For more information, see Administrators Guide and Online Help on the access point.
Authentication Tab	EAP Type	Choose **Smart Card or other Certificate**
Smart Card or other Certificate	Validate Server Certificate	Enable this option.
	Certificates	In the certificate list shown, select the certificate for this client.

Logging on to the wireless network with a WPA client using a certificate

WPA clients should now be able to connect to the access point using their TLS certificates. The certificate you installed is used when you connect, so you will not be prompted for login information. The certificate is automatically sent to the RADIUS server for authentication and authorization.

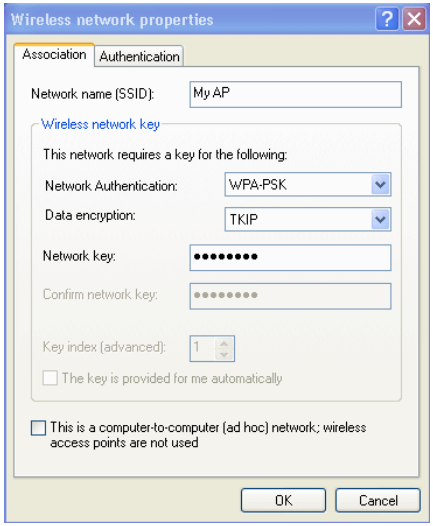
Configuring WPA-PSK security on a client

Wi-Fi Protected Access (WPA) with Pre-Shared Key (PSK) is a Wi-Fi Alliance subset of IEEE 802.11i, which includes Temporal Key Integrity Protocol (TKIP), Advanced Encryption Algorithm (AES), and Counter mode/CBC-MAC Protocol (CCMP) mechanisms. PSK employs a pre-shared key for an initial check of client credentials.

If you configured the Gateway 7001 AP to use WPA-PSK security mode, you must configure WPA-PSK security on each client.

To configure WPA-PSK security on each client:

1. On the *Network Properties* dialog box, select the **Association** tab. The *Association* dialog box opens.



2. Select **WPA-PSK** in the Network Authentication list, and **TKIP** or **AES** in the Data Encryption list, then enter a network key that matches the one specified on the access point (confirm by re-typing).

3. Click **OK** to close and save the settings.

Association Tab	Network Authentication	WPA-PSK
	Data Encryption	TKIP or AES, depending on how this option is configured on the access point. **Note:** When the Cipher Suite on the access point is set to **Both**, then TKIP clients with a valid TKIP key and AES clients with a valid CCMP (AES) key can associate with the access point. For more information, see Administrators Guide and Online Help on the access point.
	Network Key	Provide the key you entered on the access point Security settings for the cipher suite you are using. For example, if the key on the access point is set to use a TKIP key of "12345678," then a TKIP client should specify this same string as the network key.
	The key is provided for me automatically	This box should be disabled automatically, based on other settings.
Authentication Tab	Enable IEEE 802.1x authentication for this network	Make sure that IEEE 802.1x authentication is disabled (unchecked). (Setting the encryption mode to WEP should automatically disable authentication.)

Connecting to the wireless network with a WPA-PSK client

WPA-PSK clients should now be able to associate and authenticate with the access point. As a client, you will not be prompted for a key. The TKIP or AES key you configured on the client security settings is automatically used when you connect.

Configuring an external RADIUS server to recognize the Gateway 7001 AP

An external Remote Authentication Dial-in User Server (RADIUS) server running on the network can support of EAP-TLS smart card/certificate distribution to clients in a Public Key Infrastructure (PKI) as well as EAP-PEAP user account setup and authentication. By external RADIUS server, we mean an authentication server external to the access point itself. This is to distinguish between the scenario in which you use a network RADIUS server versus one in which you use the Built-in Authentication Server on the Gateway 7001 AP.

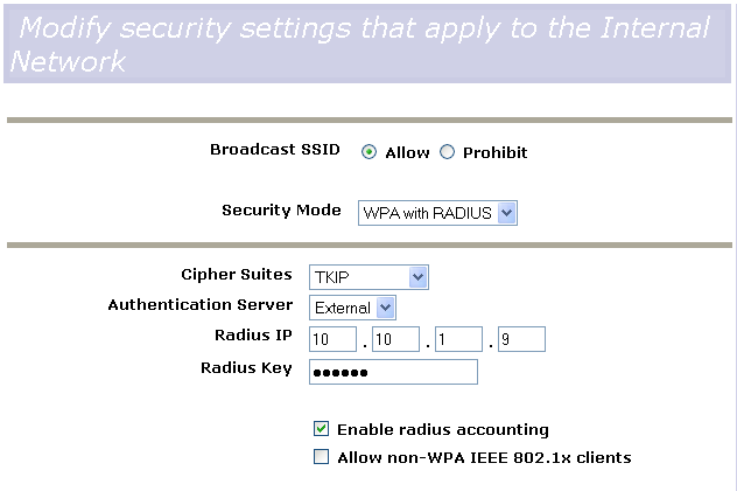
This section provides an example of configuring an external RADIUS server for the purposes of authenticating and authorizing TLS-EAP certificates from wireless clients of a particular Gateway 7001 AP configured for either "WPA with RADIUS" or "IEEE 802.1x" security modes. The intention of this section is to provide some idea of what this process will look like. Procedures will vary depending on the RADIUS server you use and how you configure it. For this example, we use the Internet Authentication Service that comes with Microsoft Windows 2003 server.

Important

This document does not describe how to set up Administrative users on the RADIUS server. In this example, we assume you already have RADIUS server user accounts configured. You will need a RADIUS server user name and password for both this procedure and the following one that describes how to obtain and install a certificate on the wireless client. Consult the documentation for your RADIUS server for information on setting up user accounts.

The purpose of this procedure is to identify your Gateway 7001 AP as a "client" to the RADIUS server. The RADIUS server can then handle authentication and authorization of wireless clients for the AP. This procedure is required for each access point. If you have more than one access point with which you plan to use an external RADIUS server, you need to follow these steps for each of those APs.

Keep in mind that the information you need to provide to the RADIUS server about the access point corresponds to settings on the access point (**Advanced** > **Security**) and vice versa. You should have already provided the RADIUS server IP Address to the AP. In the steps that follow you will provide the access point IP address to the RADIUS server. The RADIUS Key provided on the AP is the "shared secret" you will provide to the RADIUS server.

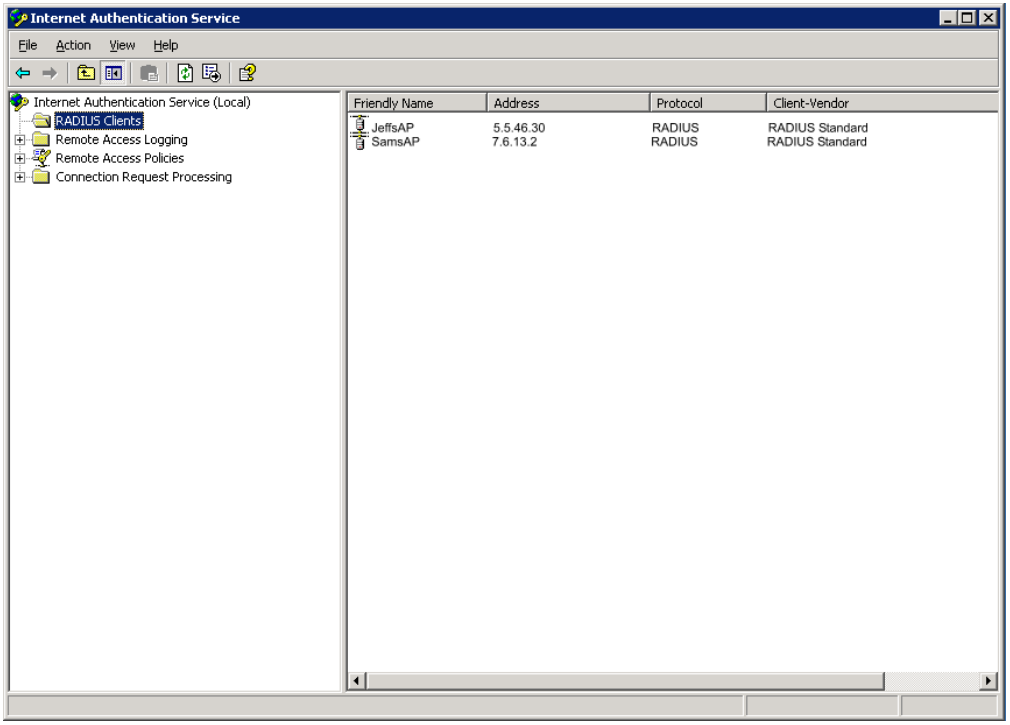


Important

The RADIUS server is identified by its IP address and UDP port numbers for the different services it provides. On the current release of the Gateway 7001 AP, the RADIUS server *User Datagram Protocol* (UDP) ports used by the access point are not configurable. (The Gateway 7001 AP is hard-coded to use RADIUS server UDP port 1812 for authentication and port 1813 for accounting.)

To identify your Gateway 7001 AP as a client to the RADIUS server:

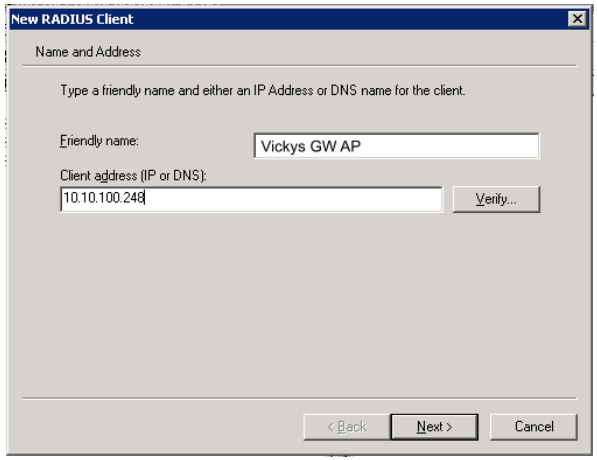
1 Log on to the system hosting your RADIUS server and open the Internet Authentication Service.



2 In the left panel, right-click the **RADIUS Clients** node and choose **New > Radius Client** from the menu.

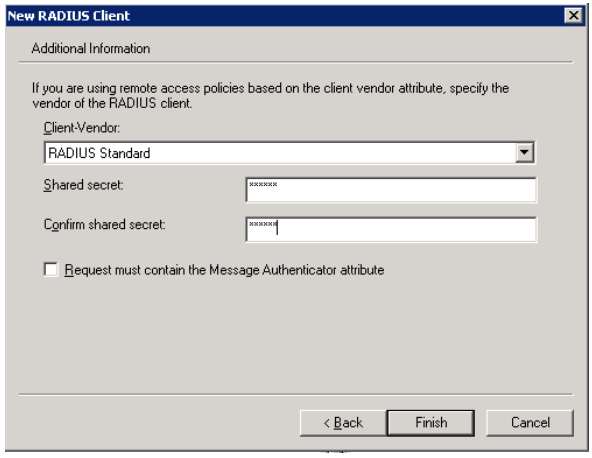
3 On the initial screen of the New RADIUS Client wizard, provide information about the Gateway 7001 AP to which you want your clients to connect:

- A logical (friendly) name for the access point. (You might want to use the DNS name or location.)
- IP address for the access point.



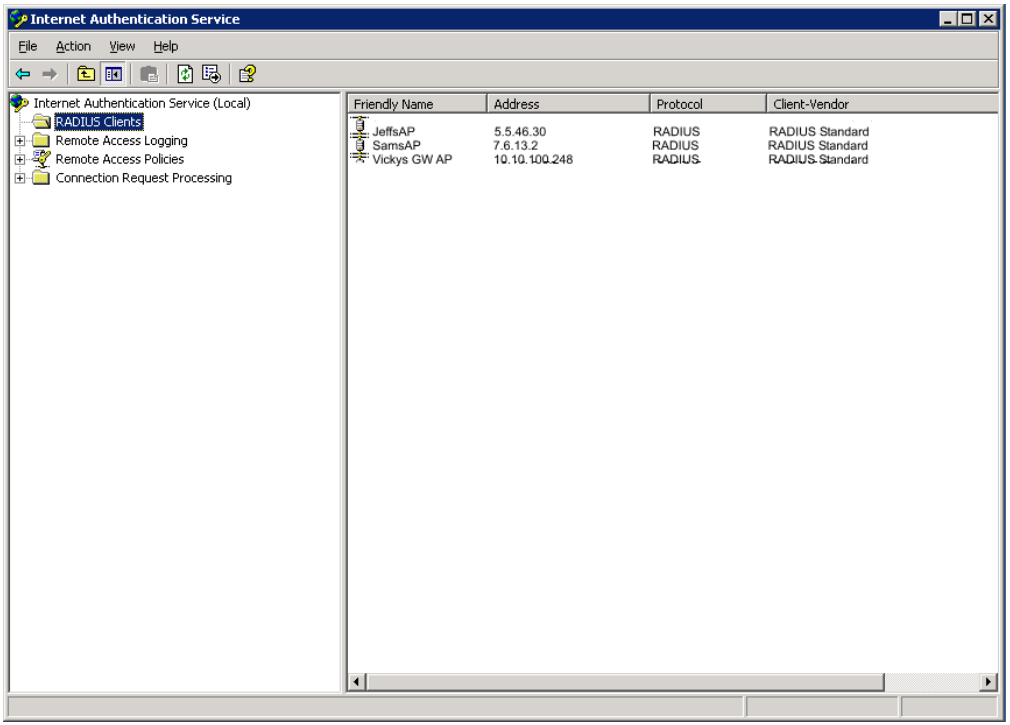
4 Click **Next**.

5 For the "Shared secret" enter the RADIUS Key you provided to the access point (on the Advanced > Security page). Re-type the key to confirm.



6 Click **Finish**.

The access point is now displayed as a client of the Authentication Server.



Obtaining a TLS-EAP certificate for a client

Important

If you want to use IEEE 802.1x mode with EAP-TLS certificates for authentication and authorization of clients, you must have an external RADIUS server and a Public Key Authority Infrastructure (PKI), including a Certificate Authority (CA), server configured on your network. It is beyond the scope of this document to describe the configuration of the RADIUS server, PKI, and CA server. Consult the documentation for those products.

Some good starting points available on the Web for the Microsoft Windows PKI software are: "How to Install/Uninstall a Public Key Certificate Authority for Windows 2000" at http://sup-port.microsoft.com/default.aspx?scid=kb;EN-US;231881 and "How to Configure a Certificate Server" at http://support.microsoft.com/default.aspx?scid=kb;en-us;318710#3.

Wireless clients configured to use either "WPA with RADIUS" or "IEEE 802.1x" security modes with an external RADIUS server that supports TLS-EAP certificates must obtain a TLS certificate from the RADIUS server. This is an initial one-time step that must be completed on each client that uses either of these modes with certificates. In this procedure, we use the Microsoft Certificate Server as an example.

To obtain a certificate for a client, follow these steps.

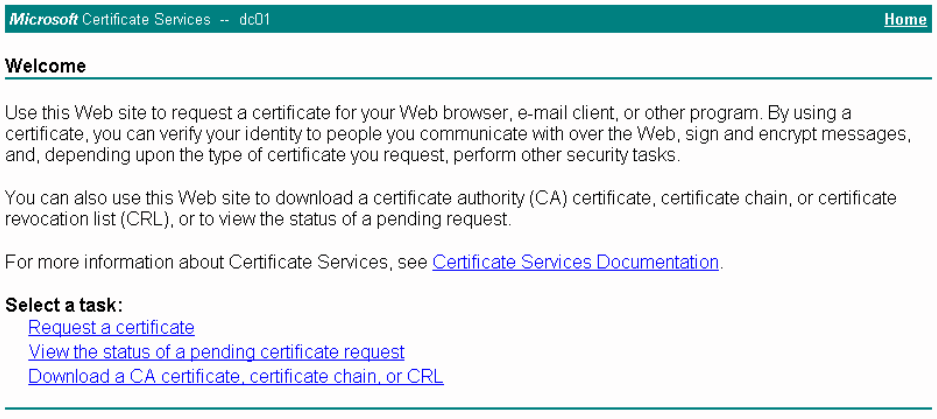
1. Go to the following URL in a Web browser:

   https://*IPAddressOfServer*/certsrv/

   Where *IPAddressOfServer* is the IP address of your external RADIUS server or of the Certificate Authority (CA), depending on the configuration of your infrastructure.

   A security alert opens.

Click **Yes** to proceed to the secure Web page for the server. The *Welcome* screen for the Certificate Server is displayed in the browser.



2 Click **Request a certificate** to get the login prompt for the RADIUS server.

3 Provide a valid user name and password to access the RADIUS server, then click **OK**.

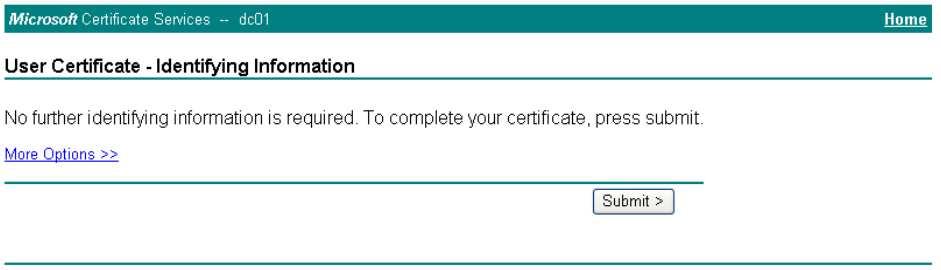
Important

The user name and password you need to provide here is for access to the RADIUS server, for which you will already have user accounts configured at this point. This document does not describe how to set up Administrative user accounts on the RADIUS server. Consult the documentation for your RADIUS server for these procedures.

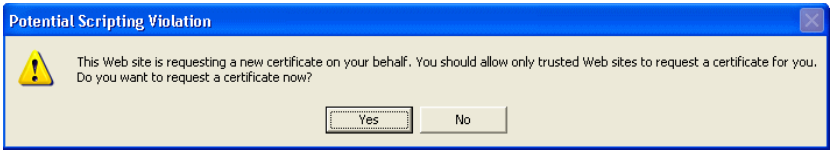
The *Request a Certificate* dialog box opens.

4 Click **User Certificate**. A *Security Warning* opens.

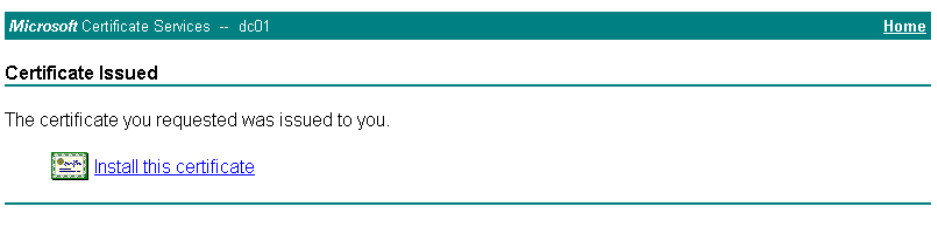
5 Click **Yes** on the dialog box displayed to install the certificate. The *User Certificate - Identifying Information* dialog box opens.



6 Click **Submit** to complete. A *Potential Security Violation* dialog box opens.



7 Click **Yes** to confirm the submittal. The *Certificate Issued* dialog box opens.



8 Click **Install this certificate** to install the newly issued certificate on your client station, Then click **Yes** on the popup windows that appear to confirm the install and to add the certificate to the Root Store.

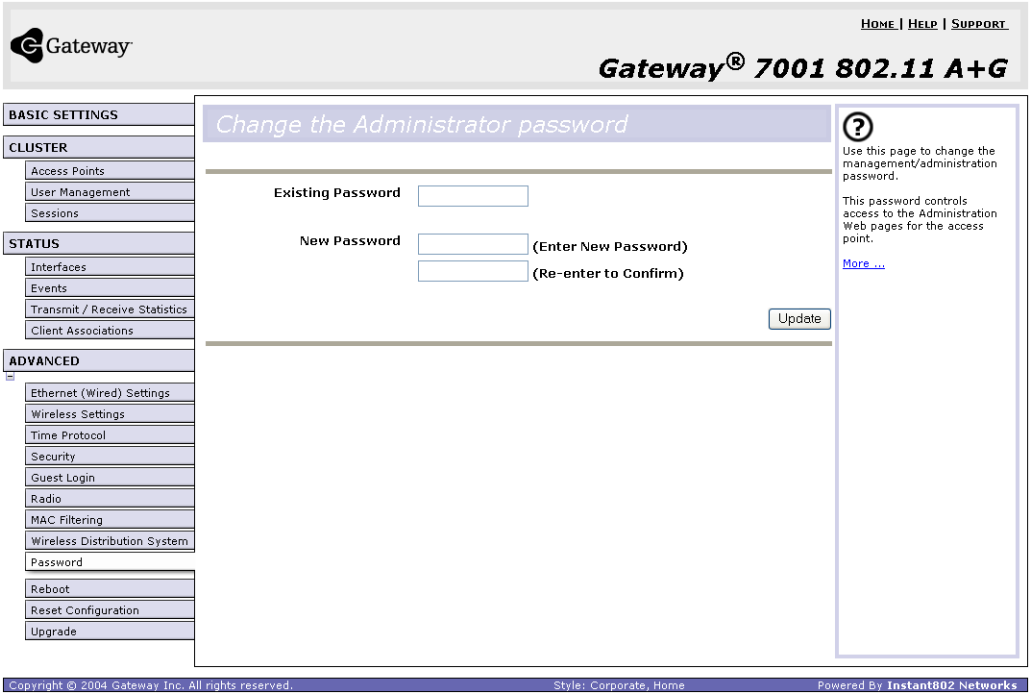
A success message is displayed indicating the certificate is now installed on the client.

Setting the administrator password

The administrator password controls access to the Administration Web pages for the Gateway 7001 Series self-managed AP. This setting is also available on the Basic Settings administration page. When you set the administrator password in either place and apply the change, the new password is updated and shared by all access points in the cluster.

Navigating to administrator password setting

To set the administrator password, click **Advanced > Password** on the *Administration* Web page. The *Change the Administrator password* screen opens. Update the boxes as described in the following section.



Setting the administrator password

To set a new administrator password, fill in the password, then re-confirm. The password setting requires that you know the existing password before you can change it. This is to prevent an unauthorized person from changing the password in a case where you leave an open browser unattended.

Field	Description
Existing Password	Type a new administrator password. The text you type will be displayed as “*” characters to prevent others from seeing your password as you type.
New Password	Re-type the new administrator password to confirm that you typed it as intended.

Updating settings

To apply your changes, click **Update**.

Chapter 8

Maintenance and Monitoring

- Interfaces
- Event log
- Transmit/receive statistics
- Associated wireless clients
- Rebooting the access point
- Resetting the configuration
- Upgrading the firmware

Introduction

The maintenance and monitoring tasks described here all pertain to viewing and modifying settings on specific access points, and not on a cluster configuration that is automatically shared by multiple access points. Therefore, it is important to ensure that you are accessing the *Administration* Web pages for the particular access point you want to configure. For information on this, see "Navigating to information for a specific AP and managing standalone APs" on page 53.

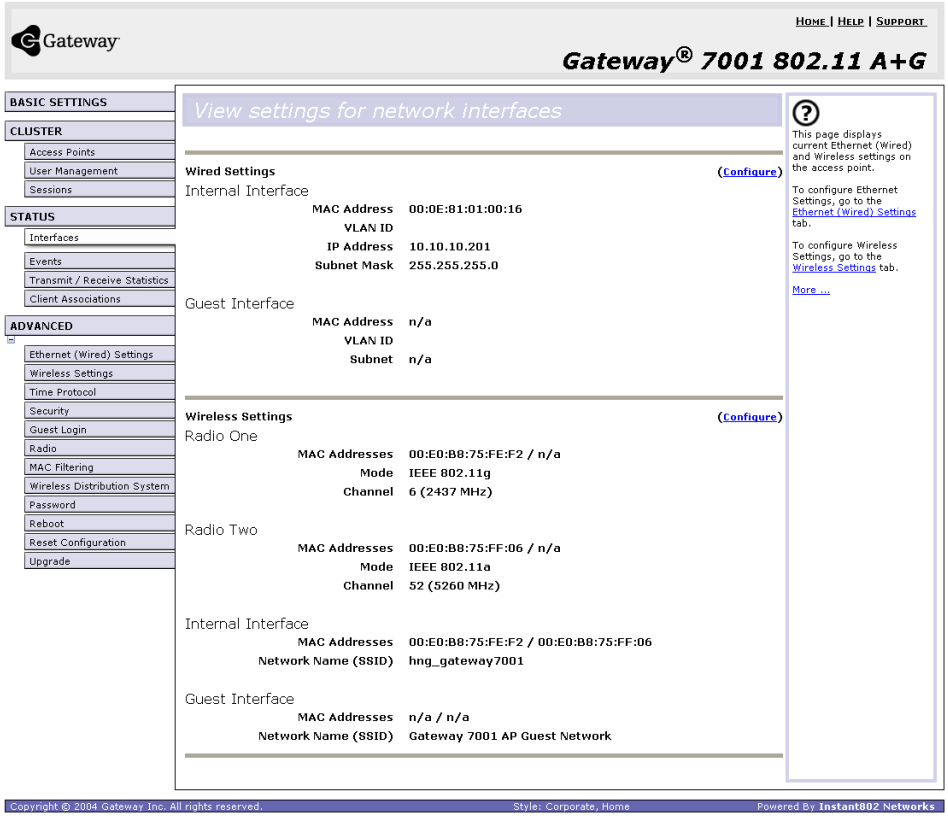
Interfaces

To monitor wired LAN and wireless LAN (WLAN) settings, select the access point you want to monitor on the *Administration* Web page, then click **Status > Interfaces**. The *View settings for network interfaces* screen opens.

Important

The dual band AP (Gateway 7001 802.11 A+G Wireless Access Point), shows current wireless settings for both Radio One and Radio Two. The single band AP (Gateway 7001 802.11 G Wireless Access Point) shows settings for one radio only.

The *Interfaces* page for the dual band AP is shown in the following figure.



This page displays the current settings of the Gateway 7001 Series self-managed AP. It displays the Ethernet (Wired) settings and the Wireless settings.

Ethernet (Wired) settings

The internal interface includes the MAC Address, IP Address, Subnet Mask, and Associated Network Wireless Name (SSID).

The guest interface includes the MAC Address, VLAN ID, and Associated Network Wireless Name (SSID).

If you want to change any of these settings, click **Configure**.

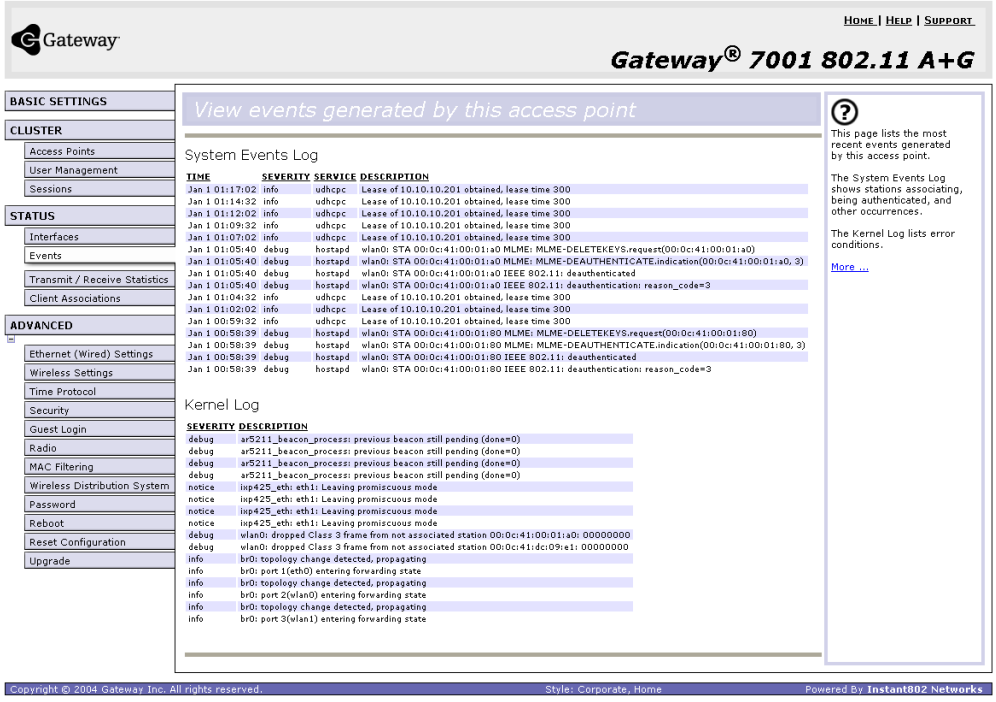
Wireless settings

The *Radio* Interface settings include the MAC Address, radio Mode, and Channel. Also shown here are MAC addresses (read-only) for internal and guest interfaces. (See "Configuring a wireless interface" on page 74 and "Configuring radio settings" on page 104 for more information.)

If you want to change any of these settings, click **Configure**.

Event log

To view transmit/receive statistics for a particular access point, select the access point you want to monitor on the *Administration* Web page, then click **Status > Events**. The *View events generated by this access point* screen opens.



This page lists the most recent events generated by this access point.

It displays the *System Events Log*, which shows stations associating, being authenticated, and other occurrences.

It provides a *Kernel Log*, which lists error conditions, such as dropping frames, and so on.

Important

The Gateway 7001 Series self-managed AP acquires its date and time information using the network time protocol (NTP). This data is reported in UTC format (also known as *Greenwich Mean Time*). You need to convert the reported time to your local time.

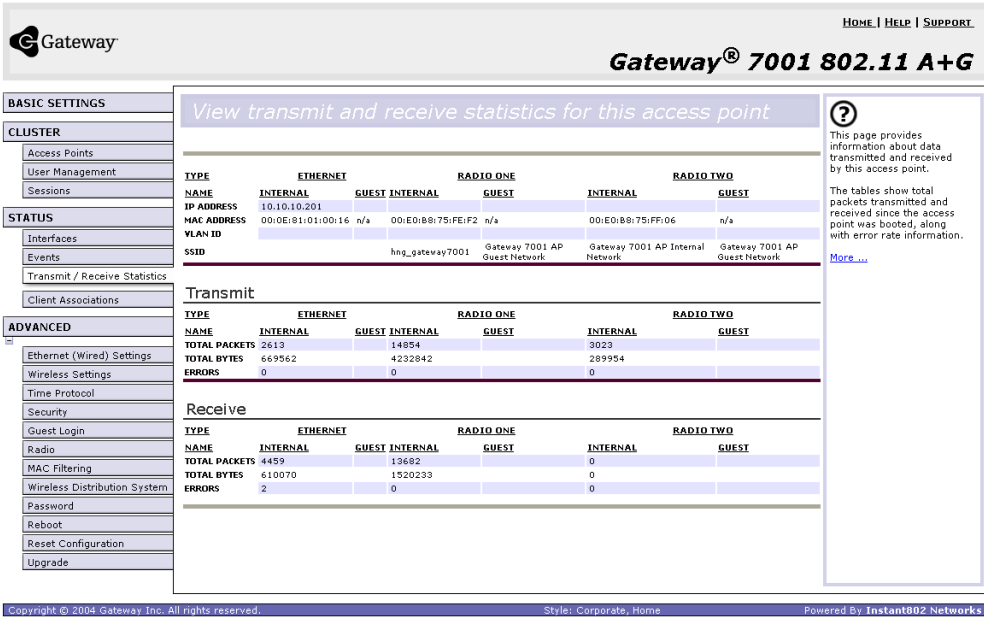
For information on setting the network time protocol, see "Enabling a network time protocol server" on page 78.

Transmit/receive statistics

To view transmit/receive statistics for a particular access point, select the access point you want to monitor on the *Administration* Web page, then click **Status > Transmit/Receive Statistics**. The *View transmit and receive statistics for this access point* screen opens.

Important

The following figure shows the Transmit / Receive page for a dual band AP (Gateway 7001 802.11 A+G Wireless Access Point). The *Administration* Web page for the single band AP (Gateway 7001 802.11 G Wireless Access Point) will look slightly different.

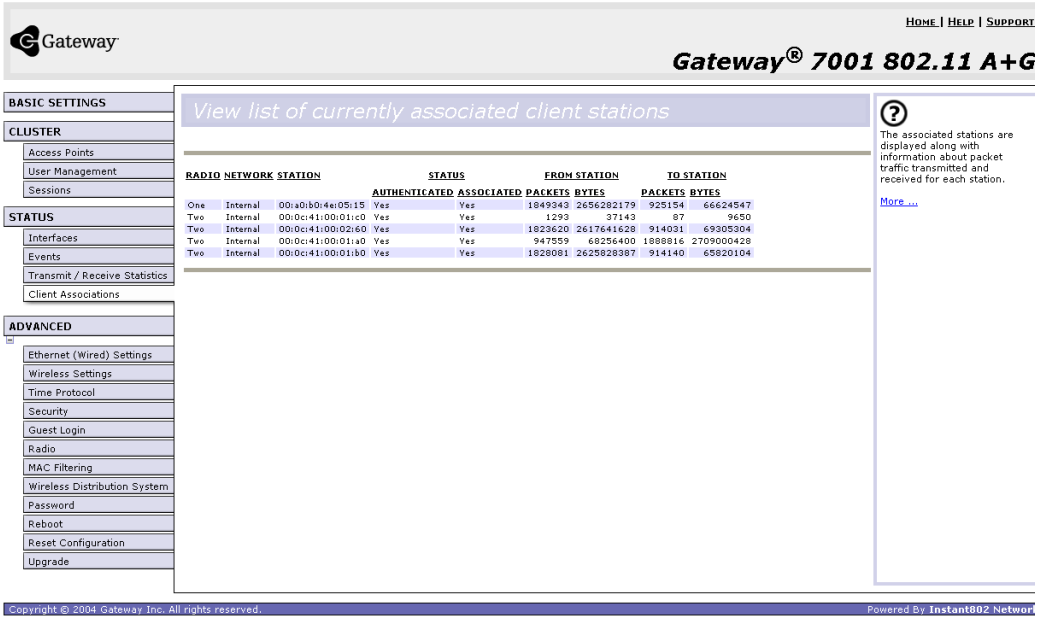


This screen provides some basic information about the current access point and a real-time display of the transmit and receive statistics for this access point as described in the following table. All transmit and receive statistics shown are totals since the access point was last started. If the AP is rebooted, these figures indicate transmit/receive totals since the re-boot.

Field	Description
IP Address	IP Address for the access point.
MAC Address	Gateway 7001 AP Administrators Guide MAC Address Media Access Control (MAC) address for the specified interface. A MAC address is a permanent, unique hardware address for any device that represents an interface to the network. The MAC address is assigned by the manufacturer. The Gateway 7001 AP has a unique MAC address for each interface. The dual-band Gateway 7001 802.11 A+G Wireless Access Point has a different MAC address for each interface on each of its two radios.
VLAN ID	Virtual LAN (VLAN) ID. A VLAN is a software-based, logical grouping of devices on a network that allow them to act as if they are connected to a single physical network, even though they may not be. VLANs can be used on the Gateway 7001 AP to establish internal and guest networks on the same access point.
SSID	Wireless network name. Also known as the SSID, this alphanumeric key uniquely identifies a wireless local area network. The SSID is set on the Basic Settings tab. (See "Providing administrator password and wireless network name" on page 32.)
Transmit and Receive Information	
Total Packets	Indicates total packets sent (in Transmit table) or received (in Received table) by this access point.
Total Bytes	Indicates total bytes sent (in Transmit table) or received (in Received table) by this access point.
Errors	Indicates total errors related to sending and receiving data on this access point.

Associated wireless clients

To view the client stations associated with a particular access point, select the access point you want to monitor on the *Administration* Web page, then click **Status > Client Associations**. The *View list of currently associated client stations* screen opens.



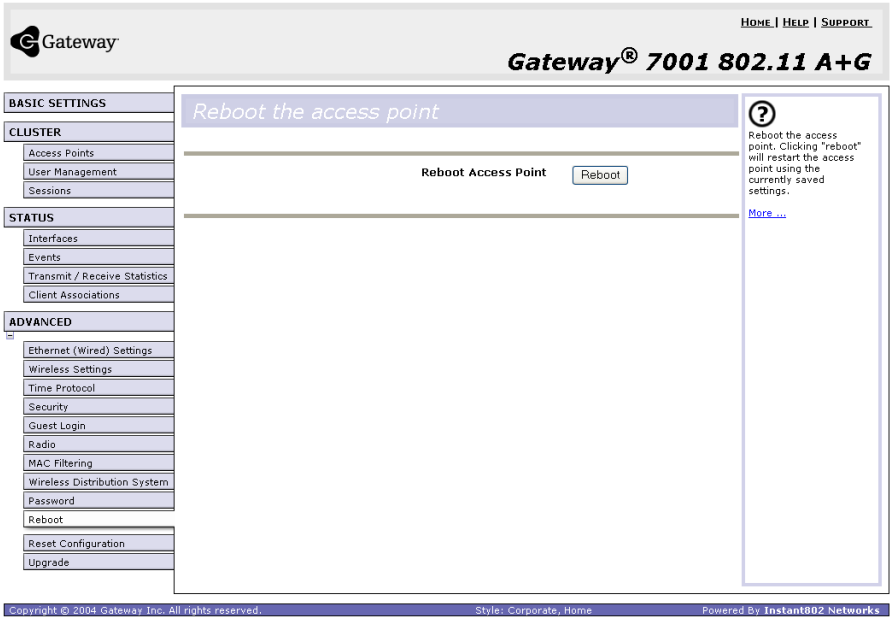
The associated stations are displayed along with information about packet traffic transmitted and received for each station.

Rebooting the access point

For maintenance purposes or as a troubleshooting measure, you can reboot the Gateway 7001 AP as follows.

To reboot the access point:

1 From the *Administration* Web page, click **Advanced > Reboot**. The *Reboot* page opens.



2 Click **Reboot**. The AP reboots.

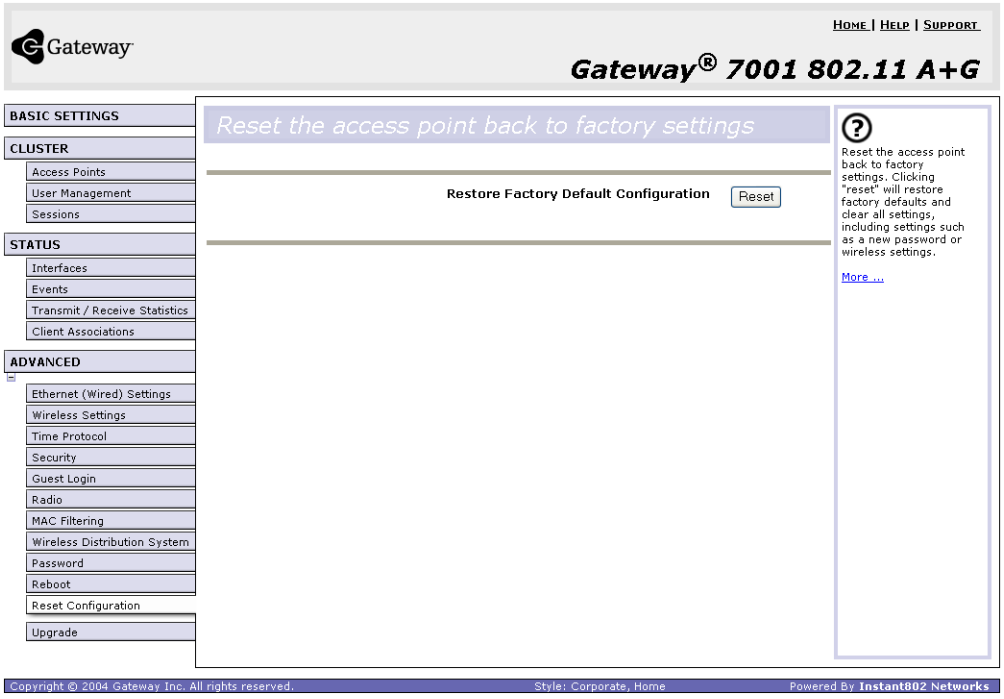
Resetting the configuration

If you are experiencing extreme problems with the Gateway 7001 Series self-managed AP and have tried all other troubleshooting measures, use the **Reset Configuration** function. This will restore factory defaults and clear all settings, including settings such as a new password or wireless settings.

As an alternative, you can also press the Reset button on the back of the AP for 15 seconds, wait until the LAN1 LED goes out, then release the button. The AP will reboot with default settings in place.

To reset the configuration:

1 From the *Administration* Web page, click **Advanced > Reset Configuration**. The *Reset the access point back to factory settings* screen opens.



2 Click **Reset**. Factory defaults are restored.

Important

Keep in mind that if you do reset the configuration from this page, you are doing so for this access point only, and not for other access points in the cluster.

For information on the factory default settings, see "Default settings and supported administrator/client platforms" on page 5.

Upgrading the firmware

As new versions of the Gateway 7001 Series self-managed AP firmware become available, you can upgrade the firmware on your access points to take advantages of new features and enhancements.

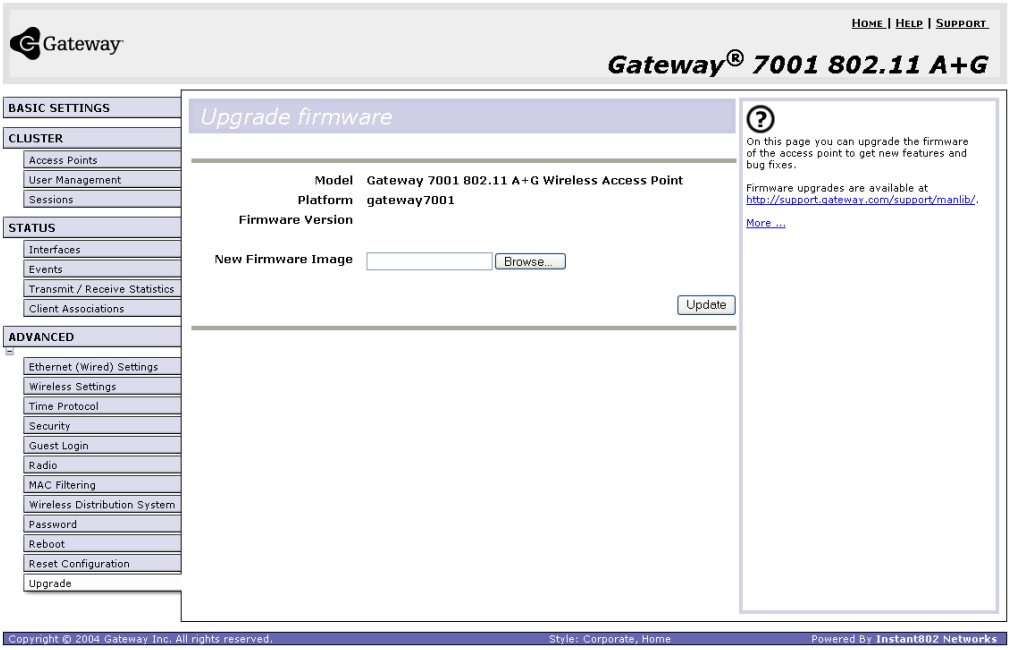
Important

You must do this for each access point. You cannot upgrade firmware automatically across the cluster.

Keep in mind that a successful firmware upgrade restores the access point configuration to the factory defaults. (See "Default settings and supported administrator/client platforms" on page 5.)

To upgrade the firmware on a particular access point:

1. Select the access point to upgrade from the *Administration* Web page, then click **Advanced > Upgrade**. The *Upgrade firmware* page for the chosen access point opens.



2. If you know the path to the new firmware image file, type it in the textbox. Otherwise, click Browse and locate the firmware image file.

3. Click **Update** to apply the new firmware image.

When clicking **Update** for the firmware upgrade, a popup confirmation window is displayed that describes the upgrade process.

Click **OK** to confirm the upgrade, and start the process

4 Repeat steps 1 to 3 for each access point you want to upgrade.

Important

To verify that the firmware upgrade completed successfully, check the firmware version shown on the **Advanced > Upgrade** tab (and also on the **Basic Settings** tab).

If the upgrade was successful, the updated version name or number will be indicated.

Chapter 9

Troubleshooting and Getting Help

- Known problems
- Technical support

Known problems

The following table summarizes problems that have been identified in the Gateway 7001 AP software.

Bug Numbers	Description	Workaround
2690, 2703	IP address for access point may change when Guest Access is enabled or when the DNS name is changed.	Use Kickstart or check DHCP logs to determine new IP address for access point.
2677, 2691, 2756	Some actions such as enabling guest access or adding a large amount of MAC addresses at once (15 or more) can corrupt the access point configuration file and prevent access to the Administration Web pages.	Physically reboot the access point by pressing the Power button on the device. (See "Cluster recovery" on page 46 for more information.)
2701, 2702, 2735, 2737, 2662, 2705	Various events or actions such as shutdown (power outage) or removal of an access point may cause problems with joining or removing an access point from the cluster, or with other aspects of a configuration sharing. Some of these problems may be indicated by a red status message at the bottom of the Administration Web page. (For example, **activator timed out.**)	Reset the access point. Navigate to Advanced > Reset Con-figuration on the access point and click the **Reset** button. (See "Cluster recovery" on page 46 for more information.)
2726, 2727	If you have more than one access point on a *Virtual LAN* (VLAN) setup, the access points cannot cluster.	Use access points in standalone mode or reconfigure without VLAN.
2654	Guest Access is not a clustered feature. However, enabling or disabling Guest Access on any one access point in a cluster configuration "partially" syncs to other cluster members. If you enable or disable Guest Access on one access point in a cluster without immediately making the same configuration change to all other cluster members, inconsistent behavior can occur. For example, this can result in a scenario where all access points are beaconing for Guest Access, but only the access point on which the change was made bridges traffic.	Either all access points in a cluster must have Guest Access enabled, or all access points in a cluster must have Guest Access disabled. Whenever you change the Guest Access status of one access point in a cluster, immediately change the Guest Access status in the same way on the other cluster members to ensure consistent operation. To enable or disable Guest Access, navigate to the Administration Web pages for each access point. If you wish to use Guest Access on only certain access points, place these access points in standalone mode.

Technical Support

Gateway offers a wide range of customer service, technical support, and information services.

Telephone numbers

You can access the following services through your telephone to get answers to your questions:

Resource	Service description	How to reach
Gateway Technical Support	Talk to a Gateway Technical Support representative about a non-tutorial technical support question.)	877-485-1464 (US) 800-846-3609 (Canada and Puerto Rico
	TDD Technical Support (for hearing impaired) is available:	605-232-2191 (all other countries)
	Weekdays 6:00 a.m. - 8:00 p.m. Central Time	800-846-1778 (TDD)
	Weekends 6:00 a.m. - 5:00 p.m. Central Time	
Sales, accounting, and warranty	Get information about available systems, pricing, orders, billing statements, warranty service, or other non-technical issues.	800-846-2000 (US) 888-888-2037 (Canada)

Appendix A

Glossary

802

IEEE 802 (IEEE Std. 802-2001) is a family of standards for peer-to-peer communication over a LAN. These technologies use a shared-medium, with information broadcast for all stations to receive. The basic communications capabilities provided are packet-based. The basic unit of transmission is a sequence of data octets (8-bits), which can be of any length within a range that is dependent on the type of LAN.

Included in the 802 family of IEEE standards are definitions of bridging, management, and security protocols.

802.1x

IEEE 802.1x (IEEE Std. 802.1x-2001) is a standard for passing EAP packets over an 802.11 wireless network using a protocol called *EAP Encapsulation Over LANs* (EAPOL). It establishes a framework that supports multiple authentication methods.

IEEE 802.1x authenticates users not machines.

802.2

IEEE 802.2 (IEEE Std. 802.2.1998) defines the LLC layer for the 802 family of standards.

802.3

IEEE 802.3 (IEEE Std. 802.3-2002) defines the MAC layer for networks that use CSMA/CA. Ethernet is an example of such a network.

802.11

IEEE 802.11 (IEEE Std. 802.11-1999) is a medium access control (MAC) and physical layer (PHY) specification for wireless connectivity for fixed, portable, and moving stations within a local area. It uses direct sequence spread spectrum (DSSS) in the 2.4 GHz ISM band and supports raw data rates of 1 and 2 Mbps. It was formally adopted in 1997 but has been mostly superseded by 802.11b.

IEEE 802.11 is also used generically to refer to the family of IEEE standards for wireless local area networks.

802.11a

IEEE 802.11a (IEEE Std. 802.11a-1999) is a PHY standard that specifies operating in the 5 GHz U-NII band using orthogonal frequency division multiplexing (OFDM). It supports data rates ranging from 6 to 54 Mbps.

802.11a Turbo

IEEE 802.11a Turbo is a proprietary variant of the 802.11a standard from Atheros Communications. It supports accelerated data rates ranging from 6 to 108Mbps.

802.11b

IEEE 802.11b (IEEE Std. 802.11b-1999) is an enhancement of the initial 802.11 PHY to include 5.5 Mbps and 11 Mbps data rates. It uses direct sequence spread spectrum (DSSS) or frequency hopping spread spectrum (FHSS) in the 2.4 GHz ISM band as well as complementary code keying (CCK) to provide the higher data rates. It supports data rates ranging from 1 to 11 Mbps.

802.11e

IEEE 802.11e is a developing IEEE standard for MAC enhancements to support QoS. It provides a mechanism to prioritize traffic within 802.11. It defines allowed changes in the Arbitration Interframe Space, a minimum and maximum Contention Window size, and the maximum length (in kμsec) of a burst of data.

IEEE 802.11e is still a draft IEEE standard (most recent version is D5.0, July 2003). A currently available subset of 802.11e is the *Wireless Multimedia Enhancements* (WME) standard.

802.11f

IEEE 802.11f (IEEE Std. 802.11f-2003) is a standard that defines the inter access point protocol (IAPP) for access points (wireless hubs) in an extended service set (ESS). The standard defines how access points communicate the associations and reassociations of their mobile stations.

802.11g

IEEE 802.11g (IEEE Std. 802.11g-2003) is a higher speed extension (up to 54 Mbps) to the 802.11b PHY, while operating in the 2.4 GHz band. It uses orthogonal frequency division multiplexing (OFDM). It supports data rates ranging from 1 to 54 Mbps.

802.11i

IEEE 802.11i is a developing IEEE standard for security in a wireless local area network (WLAN). It defines enhancements to the MAC Layer to counter the some of the weaknesses of WEP. 802.11i will incorporate 802.1x and stronger encryption techniques, such as Advanced Encryption Standard (AES).

IEEE 802.11i is still a draft IEEE standard (most recent version is D5.0, August 2003). A currently available subset of 802.11i is the Wi-Fi *Protected Access* (WPA) standard.

802.1Q

IEEE 802.1Q is the IEEE standard for *Virtual Local Area Networks* (VLANs) specific to wireless technologies.

(See http://www.ieee802.org/1/pages/802.1Q.html.) The standard addresses the problem of how to break large networks into smaller parts to prevent broadcast and multicast data traffic from consuming more bandwidth than is necessary. 802.11Q also provides for better security between segments of internal networks. The 802.1Q specification provides a standard method for inserting VLAN membership information into Ethernet frames.

Access Point

An *access point* is the communication hub for the devices on a WLAN, providing a connection or bridge between wireless and wired network devices. It supports a Wireless Networking Framework called Infrastructure Mode.

When one access point is connected to wired network and supports a set of wireless stations, it is referred to as a basic service set (BSS). An extended service set (ESS) is created by combining two or more BSSs.

Ad-hoc Mode

Ad-hoc mode is a Wireless Networking Framework in which stations communicate directly with each other. It is useful for quickly establishing a network in situations where formal infrastructure is not required.

Ad-hoc mode is also referred to as *peer-to-peer mode* or an independent basic service set (IBSS).

AES

The *Advanced Encryption Standard* (AES) is a symmetric 128-bit block data encryption technique developed to replace DES encryption. AES works at multiple network layers simultaneously.

Further information is available on the NIST Web site.

Basic Rate Set

The *basic rate set* defines the transmission rates that are mandatory for any station wanting to join this wireless network. All stations must be able to receive data at the rates listed in this set.

Beacon

Beacon frames provide the "heartbeat" of a WLAN, announcing the existence of the network, and enabling stations to establish and maintain communications in an orderly fashion. It carries the following information (some of which is optional):

- The *Timestamp* is used by stations to update their local clock, enabling synchronization among all associated stations.

- The *Beacon interval* defines the amount of time between transmitting beacon frames. Before entering power save mode, a station needs the beacon interval to know when to wake up to receive the beacon.
- The *Capability Information* lists requirements of stations that want to join the WLAN. For example, it indicates that all stations must use WEP.
- The *Service Set Identifier* (SSID).
- The *Basic Rate Set* is a bitmap that lists the rates that the WLAN supports.
- The optional *Parameter Sets* indicates features of the specific signaling methods in use (such as frequency hopping spread spectrum, direct sequence spread spectrum, etc.).
- The optional *Traffic Indication Map* (TIM) identifies stations, using power saving mode, that have data frames queued for them.

Bridge

A connection between two local area networks (LANs) using the same protocol, such as Ethernet or IEEE 802.1x.

Broadcast

A *Broadcast* sends the same message at the same time to everyone. In wireless networks, broadcast usually refers to an interaction in which the access point sends data traffic in the form of IEEE 802.1x Frames to all client stations on the network.

Some wireless security modes distinguish between how unicast, multicast, and broadcast frames are encrypted or whether they are encrypted.

See also Unicast and Multicast.

Broadcast Address

See IP Address.

BSS

A *basic service set* (BSS) is an Infrastructure Mode Wireless Networking Framework with a single access point. Also see extended service set (ESS) and independent basic service set (IBSS).

BSSID

In Infrastructure Mode, the *Basic Service Set Identifier* (BSSID) is the 48-bit MAC address of the wireless interface of the Access Point.

CCMP

Counter mode/CBC-MAC Protocol (CCMP) is an encryption method for 802.11i that uses AES. It employs a *CCM* mode of operation, combining the Cipher Block Chaining Counter mode (CBC-CTR) and the Cipher Block Chaining Message Authentication Code (CBC-MAC) for encryption and message integrity.

AES-CCMP requires a hardware coprocessor to operate.

CGI

The *Common Gateway Interface* (CGI) is a standard for running external programs from an HTTP server.

It specifies how to pass arguments to the executing program as part of the HTTP request. It may also define a set of environment variables.

A CGI program is a common way for an HTTP server to interact dynamically with users. For example, an HTML page containing a form can use a CGI program to process the form data after it is submitted.

Channel

The *Channel* defines the portion of the radio spectrum the radio uses for transmitting and receiving.

Each 802.11 standard offers a number of channels, dependent on how the spectrum is licensed by national and transnational authorities such as the Federal Communications Commission (FCC), the European Telecommunications Standards Institute (ETSI), the Korean Communications Commission, or the Telecom Engineering Center (TELEC).

CSMA/CA

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is a low-level network arbitration/ contention protocol. A station listens to the media and attempts to transmit a packet when the channel is quiet. When it detects that the channel is idle, the station transmits the packet. If it detects that the channel is busy, the station waits a random amount of time, then attempts to access the media again.

CSMA/CA is the basis of the IEEE 802.11e Distributed Control Function (DCF).

The CSMA/CA protocol used by 802.11 networks is a variation on CSMA/CD (used by Ethernet networks). In CSMA/CD the emphasis is on collision *detection* whereas with CSMA/CA the emphasis is on collision *avoidance*.

DCF

The *Distribution Control Function* is a component of the IEEE 802.11e Quality of Service (QoS) technology standard. The DCF coordinates channel access among multiple stations on a wireless network by controlling wait times for channel access. Wait times are determined by a random backoff timer which is configurable by defining minimum and maximum contention windows.

DHCP

The *Dynamic Host Configuration Protocol* (DHCP) is a protocol specifying how a central server can dynamically provide network configuration information to clients. A DHCP server "offers" a "lease" (for a pre-configured period of time—see Lease Time) to the client system. The information supplied includes the client's IP addresses and net mask plus the address of its DNS servers and Gateway.

DNS

The *Domain Name Service* (DNS) is a general-purpose query service used for translating fully-qualified names into Internet addresses. A fully-qualified name consists of the hostname of a system plus its domain name.

A *domain name* identifies one or more IP addresses. Conversely, an IP address may map to more than one domain name.

A domain name has a suffix that indicates which top level domain (TLD) it belongs to. Every country has its own top-level domain, for example .de for Germany, .fr for France, .jp for Japan, .tw for Taiwan, .uk for the United Kingdom, .us for the U.S.A., and so on. There are also .com for commercial bodies, .edu for educational institutions, .net for network operators, and .org for other organizations as well as .gov for the U. S. government and .mil for its armed services.

DOM

The *Document Object Model* (DOM) is an interface that lets programs and scripts dynamically access and update the content, structure, and style of documents. The DOM lets you model the objects in an HTML or XML document (text, links, images, tables), defining the attributes of each object and how they can be manipulated.

Further details about the DOM can be found at the W3C.

DTIM

The *Delivery Traffic Information Map* (DTIM) message is an element included in some Beacon frames. It indicates which stations, currently sleeping in low-power mode, have data buffered on the Access Point awaiting pick-up. Part of the DTIM message indicates how frequently stations must check for buffered data.

Dynamic IP Address

See IP Address.

EAP

The *Extensible Authentication Protocol* (EAP) is an authentication protocol that supports multiple methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication, and smart cards.

Variations on EAP include EAP Cisco Wireless (LEAP), Protected EAP (PEAP), EAP-TLS, and EAP Tunnelled TLS (EAP-TTLS).

ESS

An *extended service set* (ESS) is an Infrastructure Mode Wireless Networking Framework with multiple access points, forming a single subnetwork that can support more clients than a basic service set (BSS).

Each access point supports a number of wireless stations, providing broader wireless coverage for a large space, for example, an office.

Ethernet

Ethernet is a local-area network (LAN) architecture supporting data transfer rates of 10 Mbps to 1 Gbps.

The Ethernet specification is the basis for the IEEE 802.3 standard, which specifies the physical and lower software layers. It uses the CSMA/CA access method to handle simultaneous demands.

Ethernet supports data rates of 10 Mbps, *Fast Ethernet* supports 100 Mbps, and *Gigabit Ethernet* supports 1 Gbps. Its cables are classified as "*X*base*Y*", where *X* is the data rate in Mbps and *Y* is the category of cabling. The original cable was *10base5* (Thicknet or "Yellow Cable"). Some others are *10base2* (Cheapernet), *10baseT* (Twisted Pair), and *100baseT* (Fast Ethernet). The latter two are commonly supplied using *CAT5* cabling with *RJ-45* connectors. There is also *1000baseT* (Gigabit Ethernet).

Frame

A Frame consists of a discrete portion of data along with some descriptive meta-information packaged for transmission on a wireless network. Each frame includes a source and destination MAC address, a control field with protocol version, frame type, frame sequence number, frame body (with the actual information to be transmitted) and frame check sequence for error detection. A Frame is similar in concept to a Packet, the difference being that a packet operates on the Network layer (layer 3 in the OSI model) whereas a frame operates on the Data-Link layer (layer 2 in the OSI model).

Gateway

A *gateway* is a network node that serves as an entrance to another network. A gateway also often provides a proxy server and a firewall. It is associated with both a router, which use headers and forwarding tables to determine where packets are sent, and a switch or bridge, which provides the actual path for the packet in and out of the gateway.

Before a host on a LAN can access the Internet, it needs to know the address of its *default gateway*.

HTML

The *Hypertext Markup Language* (HTML) defines the structure of a document on the World Wide Web. It uses tags and attributes to hint about a layout for the document.

An HTML document starts with an <html> tag and ends with a </html> tag. A correctly formatted document also contains a <head> ... </head> section, which contains the metadata to define the document, and a <body> ... </body> section, which contains its content. Its markup is derived from the Standard Generalized Markup Language (SGML), which is defined in ISO 8879:1986.

HTML documents are sent from server to browser through HTTP. Also see XML.

HTTP

The *Hypertext Transfer Protocol* (HTTP) defines how messages are formatted and transmitted on the World Wide Web. An HTTP message consists of a URL and a command (GET, HEAD, POST, and so on), a request followed by a response.

IAPP

The *Inter Access Point Protocol* (IAPP) is an IEEE standard (802.11f) that defines communication between the access points in a "distribution system". This includes the exchange of information about mobile stations and the maintenance of bridge forwarding tables, plus securing the communications between access points.

IBSS

An *independent basic service set* (IBSS) is an Ad-hoc Mode Wireless Networking Framework in which stations communicate directly with each other.

IEEE

The Institute of Electrical and Electronic Engineers (IEEE) is an international standards body that develops and establishes industry standards for a broad range of technologies, including the 802 family of networking and wireless standards. (See 802, 802.1x, 802.11, 802.11a, 802.11b, 802.11e, 802.11f, 802.11g, and 802.11i.)

For more information about IEEE task groups and standards, see http://standards.ieee.org/.

Infrastructure Mode

Infrastructure Mode is a Wireless Networking Framework in which wireless stations communicate with each other by first going through an Access Point. In this mode, the wireless stations can communicate with each other or can communicate with hosts on a wired network. The access point is connected to a wired network and supports a set of wireless stations.

An infrastructure mode framework can be provided by a single access point (BSS) or a number of access points (ESS).

Intrusion Detection

The *Intrusion Detection System* (IDS) inspects all inbound network activity and reports suspicious patterns that may indicate a network or system attack from someone attempting to break into the system. It reports access attempts using unsupported or known insecure protocols.

IP

The *Internet Protocol* (IP) specifies the format of packets, also called datagrams, and the addressing scheme. IP is a connectionless, best-effort packet switching protocol. It provides packet routing, fragmentation and re-assembly. It is combined with higher-level protocols, such as TCP or UDP, to establish the virtual connection between destination and source.

The current version of IP is *IPv4*. A new version, called IPv6 or IPng, is under development. IPv6 is an attempt to solve the shortage of IP addresses.

IP Address

Systems are defined by their *IP address*, a four-byte (octet) number uniquely defining each host on the Internet. It is usually shown in form 192.168.2.254. This is called dotted-decimal notation.

An IP address is partitioned into two portions: the network prefix and a host number on that network. A Subnet Mask is used to define the portions. There are two special host numbers:

- The Network Address consists of a host number that is all zeroes (for example, 192.168.2.0).
- The Broadcast Address consists of a host number that is all ones (for example, 192.168.2.255).

There are a finite number of IP addresses that can exist. Therefore, a local area network typically uses one of the IANA-designated address ranges for use in private networks. These address ranges are:

10.0.0.0 to 10.255.255.255

172.16.0.0 to 172.31.255.255

192.168.0.0 to 192.168.255.255

A Dynamic IP Address is an IP address that is automatically assigned to a host by a DHCP server or similar mechanism. It is called dynamic because you may be assigned a different IP address each time you establish a connection.

A Static IP Address is an IP address that is hard-wired for a specific host. A static address is usually required for any host that is running a server, for example, a Web server.

IPSec

IP Security (IPSec) is a set of protocols to support the secure exchange of packets at the IP layer. It uses shared public keys. There are two encryption modes: Transport and Tunnel.

- *Transport mode* encrypts only the data portion (payload) of each packet, but leaves the headers untouched.
- The more secure *Tunnel mode* encrypts both the header and the payload.

ISP

An *Internet Service Provider* (ISP) is a company that provides access to the Internet to individuals and companies. It may provide related services such as virtual hosting, network consulting, Web design, etc.

Jitter

Jitter is the difference between the latency (or delay) in packet transmission from one node to another across a network. If packets are not transmitted at a consistent rate (including Latency), QoS for some types of data can be affected. For example, inconsistent transmission rates can cause distortion in VoIP and streaming media. QoS is designed to reduce jitter along with other factors that can impact network performance.

Latency

Latency, also known as *delay*, is the amount of time it takes to transmit a Packet from sender to receiver.

Latency can occur when data is transmitted from the access point to a client and vice versa. It can also occur when data is transmitted from access point to the Internet and vice versa. Latency is caused by *fixed network* factors such as the time it takes to encode and decode a packet, and also by *variable network* factors such as a busy or overloaded network. QoS features are designed to minimize latency for high priority network traffic.

LAN

A *Local Area Network* (LAN) is a communications network covering a limited area, for example, the computers in your home that you want to network together or a couple of floors in a building. A LAN connects multiple computers and other network devices such as storage and printers. Ethernet is the most common technology implementing a LAN.

Wireless Ethernet (802.11) is another very popular LAN technology (also see WLAN).

LDAP

The *Lightweight Directory Access Protocol* (LDAP) is a protocol for accessing on-line directory services. It is used to provide an authentication mechanism. It is based on the X.500 standard, but less complex.

Lease Time

The *Lease Time* specifies the period of time the DHCP Server gives its clients an IP Address and other required information. When the lease expires, the client must request a new lease. If the lease is set to a short span, you can update your network information and propagate the information provided to the clients in a timely manner.

LLC

The *Logical Link Control* (LLC) layer controls frame synchronization, flow control, and error checking. It is a higher level protocol over the PHY layer, working in conjunction with the MAC layer.

MAC

The *Media Access Control* (MAC) layer handles moving data packets between NICs across a shared channel. It is a higher level protocol over the PHY layer. It provides an arbitration mechanism in an attempt to prevent signals from colliding.

It uses a hardware address, known as the *MAC address*, that uniquely identifies each node of a network.

IEEE 802 network devices share a common 48-bit MAC address format, displayed as a string of twelve (12) hexadecimal digits separated by colons, for example FE:DC:BA:09:87:65.

MSCHAP V2

Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAP V2) provides authentication for PPP connections between a Windows-based computer and an Access Point or other network access device.

MTU

The *Maximum Transmission Unit* is the largest physical packet size, measured in bytes, that a network can transmit. Any messages larger than the MTU are fragmented into smaller packets before being sent.

Multicast

A *Multicast* sends the same message to a select group of recipients. Sending an e-mail message to a mailing list is an example of multicasting. In wireless networks, multicast usually refers to an interaction in which the access point sends data traffic in the form of IEEE 802.1x Frames to a specified set of client stations (MAC addresses) on the network.

Some wireless security modes distinguish between how unicast, multicast, and broadcast frames are encrypted or whether they are encrypted.

See also Unicast and Broadcast.

NAT

Network Address Translation is an Internet standard that masks the internal IP addresses being used in a LAN. A NAT server running on a gateway maintains a translation table that maps all internal IP addresses in outbound requests to its own address and converts all inbound requests to the correct internal host.

NAT serves three main purposes: it provides security by obscurity by hiding internal IP addresses, enables the use of a wide range of internal IP addresses without fear of conflict with the addresses used by other organizations, and it allows the use of a single Internet connection.

Network Address

See IP Address.

NIC

A *Network Interface Card* is an adapter or expansion board inserted into a computer to provide a physical connection to a network. Most NICs are designed for a particular type of network, protocol, and media, for example, Ethernet or wireless.

NTP

The *Network Time Protocol* assures accurate synchronization of the system clocks in a network of computers. NTP servers transmit *Coordinated Universal Time* (UTC, also known as *Greenwich Mean Time*) to their client systems. An NTP client sends periodic time requests to servers, using the returned time stamp to adjust its clock.

OSI

The *Open Systems Interconnection* (OSI) reference model is a framework for network design. The OSI model consists of seven layers:

- Layer 1, the Physical layer, identifies the physical medium used for communication between nodes.
- In the case of wireless networks, the physical medium is air, and radio frequency (RF) waves are a components of the physical layer.
- Layer 2, the Data-Link layer, defines how data for transmission will be structured and formatted, along with low-level protocols for communication and addressing. For example, protocols such as CSMA/CA and components like MAC addresses, and Frames are all defined and dealt with as a part of the Data-Link layer.
- Layer 3, the Network layer, defines the how to determine the best path for information traversing the network. Packets and logical IP Addresses operate on the network layer.
- Layer 4, the Transport layer, defines connection oriented protocols such as TCP and UDP.

- Layer 5, the Session layer, defines protocols for initiating, maintaining, and ending communication and transactions across the network. Some common examples of protocols that operate on this layer are network file system (NFS) and structured query language (SQL). Also part of this layer are communication flows like single mode (device sends information bulk), half-duplex mode (devices take turns transmitting information in bulk), and full-duplex mode (interactive, where devices transmit and receive simultaneously).
- Layer 6, the Presentation layer, defines how information is presented to the application. It includes meta-information about how to encrypt/decrypt and compress/decompress the data. JPEG and TIFF file formats are examples of protocols at this layer.
- Layer 7, the Application layer, includes protocols like hypertext transfer protocol (HTTP), simple mail transfer protocol (SMTP), and file transfer protocol (FTP).

Packet

Data and media are transmitted among nodes on a network in the form of *packets*. Data and multimedia content is divided up and packaged into *packets*. A packet includes a small chunk of the content to be sent along with its destination address and sender address. Packets are pushed out onto the network and inspected by each node. The node to which it is addressed is the ultimate recipient.

Packet Loss

Packet Loss describes the percentage of packets transmitted over the network that did not reach their intended destination. A 0 percent package loss indicates no packets were lost in transmission. QoS features are designed to minimize packet loss.

PHY

The *Physical Layer* (PHY) is the lowest layer in the network layer model (see OSI). The Physical Layer conveys the bit stream - electrical impulse, light or radio signal -- through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a medium, including defining cables, NICs, and physical aspects.

Ethernet and the 802.11 family are protocols with physical layer components.

PID

The *Process Identifier* (PID) is an integer used by Linux to uniquely identify a process. A PID is returned by the fork()system call. It can be used by wait() or kill() to perform actions on the given process.

Port Forwarding

Port Forwarding creates a 'tunnel' through a firewall, allowing users on the Internet access to a service running on one of the computers on your LAN, for example, a Web server, an FTP or SSH server, or other services. From the outside user's point of view, it looks like the service is running on the firewall.

PPP

The *Point-to-Point Protocol* is a standard for transmitting network layer datagrams (IP packets) over serial point-to-point links. PPP is designed to operate both over asynchronous connections and bit-oriented synchronous systems.

PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) is a specification for connecting the users on a LAN to the Internet through a common broadband medium, such as a single DSL or cable modem line.

PPtP

Point-to-Point Tunneling Protocol (PPtP) is a technology for creating a *Virtual Private Network* (VPN) within the *Point-to-Point Protocol* (PPP). It is used to make sure that data transmitted from one VPN node to another are secure.

Proxy

A *proxy* is server located between a client application and a real server. It intercepts requests, attempting to fulfill them itself. If it cannot, it forwards them to the real server. Proxy servers have two main purposes: improve performance by spreading requests over several machines and filter requests to prevent access to specific servers or services.

PSK

Pre-Shared Key (PSK), see Shared Key.

Public Key

A *public key* is used in public key cryptography to encrypt a message which can only be decrypted with the recipient's private or secret key. Public key encryption is also called asymmetric encryption, because it uses two keys, or Diffie-Hellman encryption. Also see Shared Key.

QoS

Quality of Service (QoS) defines the performance properties of a network service, including guaranteed throughput, transit delay, and priority queues. QoS is designed to minimize Latency, Jitter, Packet Loss, and network congestion, and provide a way of allocating dedicated bandwidth for high priority network traffic.

The IEEE standard for implementing QoS on wireless networks is currently in-work by the 802.11e task group. A subset of 802.11e features is described in the WME specification.

RADIUS

The *Remote Authentication Dial-In User Service* (RADIUS) provides an authentication and accounting system. It is a popular authentication mechanism for many ISPs.

RC4

A symmetric stream cipher provided by RSA Security. It is a variable key-size stream cipher with byte oriented operations. It allows keys up to 2048 bits in length.

Router

A *router* is a network device which forwards packets between networks. It is connected to at least two networks, commonly between two local area networks (LANs) or between a LAN and a wide-area network (WAN), for example, the Internet. Routers are located at gateways—places where two or more networks connect.

A router uses the content of headers and its tables to determine the best path for forwarding a packet. It uses protocols such as the *Internet Control Message Protocol* (ICMP), *Routing Information Protocol* (RIP), and *Internet Router Discovery Protocol* (IRDP) to communicate with other routers to configure the best route between any two hosts. The router performs little filtering of data it passes.

RSSI

The *Received Signal Strength Indication* (RSSI) an 802.1x value that calculates voltage relative to the received signal strength. RSSI is one of several ways of measuring and indicating *radio frequency* (RF) signal strength. Signal strength can also be measured in mW (milliwatts), dBms (decibel milliwatts), and a percentage value.

RTS

A *request to send* (RTS) is a message sent by a client station to the access point, asking permission to send a data packet.

RTS Threshold

The *RTS threshold* specifies the packet size of a request to send (RTS) transmission. This helps control traffic flow through the access point, and is especially useful for performance tuning on an access point with a many clients.

Shared Key

A *shared key* is used in conventional encryption where one key is used both for encryption and decryption. It is also called *secret-key* or *symmetric-key* encryption.

Also see Public Key.

SNMP

The *Simple Network Management Protocol* (SNMP) was developed to manage and monitor nodes on a network. It is part of the TCP/IP protocol suite.

SNMP consists of managed devices and their agents, and a management system. The agents store data about their devices in *Management Information Bases* (MIBs) and return this data to the SNMP management system when requested.

SSID

The *Service Set Identifier* (SSID) is a thirty-two character alphanumeric key that uniquely identifies a wireless local area network. It is also referred to as the *Network Name*. There are no restrictions on the characters that may be used in an SSID.

Static IP Address

See IP Address.

STP

The *Spanning Tree Protocol* (STP) an IEEE 802.1x standard protocol for MAC bridges that manages path redundancy and prevents undesirable loops in the network created by multiple active paths between client stations. Loops occur when there multiple routes between access points. STP creates a tree that spans all of the switches in an extended network, forcing redundant paths into a standby, or blocked, state. STP allows only one active path at a time between any two network devices (this prevents the loops) but establishes the redundant links as a backup if the initial link should fail. If STP costs change, or if one network segment in the STP becomes unreachable, the spanning tree algorithm reconfigures the spanning tree topology and reestablishes the link by activating the standby path. Without spanning tree in place, it is possible that both connections may be simultaneously live, which could result in an endless loop of traffic on the LAN

Subnet Mask

A Subnet Mask is a number that defines which part of an IP address is the network address and which part is a host address on the network. It is shown in dotted-decimal notation (for example, a 24-bit mask is shown as 255.255.255.0) or as a number appended to the IP address (for example, 192.168.2.0/24).

The subnet mask lets a router quickly determine if an IP address is local or needs to be forwarded by performing a bitwise AND operation on the mask and the IP address. For example, if an IP address is 192.168.2.128 and the net mask is 255.255.255.0, the resulting Network address is 192.168.2.0.

The bitwise AND operator compares two bits and assigns 1 to the result only if both bits are 1. The following table shows the details of the net mask:

Supported Rate Set

The *supported rate set* defines the transmission rates that are available on this wireless network. A station may be able to receive data at any of the rates listed in this set. All stations must be able to receive data at the rates listed in the Basic Rate Set.

TCP

The *Transmission Control Protocol* (TCP) is built on top of Internet Protocol (IP). It adds reliable communication (guarantees delivery of data), flow-control, multiplexing (more than one simultaneous connection), and connection-oriented transmission (requires the receiver of a packet to acknowledge receipt to the sender). It also guarantees that packets will be delivered in the same order in which they were sent.

IP address	192.168.2.128	11000000 10101000 00000010 10000000
net mask	255.255.255.0	11111111 11111111 11111111 00000000
Resulting network address	192.168.2.0	11000000 10101000 00000010 00000000

TCP/IP

The Internet and most local area networks are defined by a group of protocols. The most important of these is the *Transmission Control Protocol over Internet Protocol* (TCP/IP), the de facto standard protocols. TCP/IP was originally developed by Defense Advanced Research Projects Agency (DARPA, also known as ARPA, an agency of the US Department of Defense).

Although TCP and IP are two specific protocols, TCP/IP is often used to refer to the entire protocol suite based on these, including ICMP, ARP, UDP, and others, as well as applications that run on these protocols, such as telnet, FTP, etc.

TKIP

The *Temporal Key Integrity Protocol* (TKIP) provides an extended 48-bit initialization vector, per-packet key construction and distribution, a Message Integrity Code (MIC, sometimes called "Michael"), and a re-keying mechanism. It uses a RC4 stream cipher to encrypt the frame body and CRC of each 802.11 frame before transmission. It is an important component of the WPA and 802.11i security mechanisms.

ToS

TCP/IP packet headers include a 3-to-5 bit *Type of Service* (ToS) box set by the application developer that indicates the appropriate type of service for the data in the packet. The way the bits are set determines whether the packet is queued for sending with minimum delay, maximum throughput, low cost, or mid-way "best-effort" settings depending on the requirements of the data. The ToS box is used by the Gateway 7001 Series self-managed AP to provide configuration control over *Quality of Service* (QoS) queues for data transmitted from the AP to client stations.

UDP

The *User Datagram Protocol* (UDP) is a transport layer protocol providing simple but unreliable datagram services. It adds port address information and a checksum to an IP packet.

UDP neither guarantees delivery nor does it require a connection. It is lightweight and efficient. All error processing and retransmission must be performed by the application program.

Unicast

A *Unicast* sends a message to a single, specified receiver. In wireless networks, unicast usually refers to an interaction in which the access point sends data traffic in the form of IEEE 802.1x Frames directly to a single client station MAC address on the network.

Some wireless security modes distinguish between how unicast, multicast, and broadcast frames are encrypted or whether they are encrypted.

See also Multicast and Broadcast.

URL

A *Uniform Resource Locator* (URL) is a standard for specifying the location of objects on the Internet, such as a file or a newsgroup. URLs are used extensively in HTML documents to specify the target of a hyperlink which is often another HTML document (possibly stored on another computer). The first part of the URL indicates what protocol to use and the second part specifies the IP address or the domain name where that resource is located.

VLAN

A *virtual* LAN (VLAN) is a software-based, logical grouping of devices on a network that allow them to act as if they are connected to a single physical network, even though they may not be. The nodes in a VLAN share resources and bandwidth, and are isolated on that network. The Gateway 7001 Series Self-Managed AP supports the configuration of a wireless VLAN. This technology is leveraged on the access point for the "virtual" guest network feature.

VPN

A *Virtual Private Network* (VPN) is a network that uses the Internet to connect its nodes. It uses encryption and other mechanisms to make sure that only authorized users can access its nodes and that data cannot be intercepted.

WAN

A *Wide Area Network* (WAN) is a communications network that spans a relatively large geographical area, extending over distances greater than one kilometer. A WAN is often connected through public networks, such as the telephone system. It can also be connected through leased lines or satellites.

The Internet is essentially a very large WAN.

WDS

A *Wireless Distribution System* (WDS) allows the creation of a completely wireless infrastructure.

Typically, an Access Point is connected to a wired LAN. WDS lets access points be connected wirelessly. The access points can function as wireless repeaters or bridges.

WEP

Wired Equivalent Privacy (WEP) is a data encryption protocol for 802.11 wireless networks. All wireless stations and access points on the network are configured with a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared Key for data encryption. It uses a RC4 stream cipher to encrypt the frame body and CRC of each 802.11 frame before transmission.

Wi-Fi

A test and certification of interoperability for WLAN products based on the IEEE 802.11 standard promoted by the Wi-Fi Alliance, a non-profit trade organization.

WINS

The *Windows Internet Naming Service* (WINS) is a server process for resolving Windows-based computer names to IP addresses. It provides information that lets these systems browse remote networks using the *Network Neighborhood*.

Wireless Networking Framework

There are two ways of organizing a wireless network:

- Stations communicate directly with one another in an Ad-hoc Mode network, also known as an independent basic service set (IBSS).
- Stations communicate through an Access Point in an Infrastructure Mode network. A single access point creates an infrastructure basic service set (BSS) whereas multiple access points are organized in an extended service set (ESS).

WLAN

Wireless Local Area Network (WLAN) is a LAN that uses high-frequency radio waves rather than wires to communicate between its nodes.

WME

Wireless Multimedia Enhancements (WME) is a subset of the 802.11e draft specification. It uses four priority queues between an Access Point and its clients. WME provides an interim, standards-based QoS solution.

WPA

Wi-Fi Protected Access (WPA) is a Wi-Fi Alliance version of the draft IEEE 802.11i standard. It provides more sophisticated data encryption than WEP and also provides user authentication. WPA includes TKIP and 802.1x mechanisms.

WRAP

Wireless Robust Authentication Protocol (WRAP) is an encryption method for 802.11i that uses AES but another encryption mode (OCB) for encryption and integrity.

XML

The *Extensible Markup Language* (XML) is a specification developed by the W3C. XML is a simple, flexible text format derived from Standard Generalized Markup Language (SGML), which is defined in ISO8879:1986, designed especially for electronic publishing.

Appendix B

Specifications

Gateway	Yes	No	Comments
Supports Infrastructure Mode	X		
Supports Ad-Hoc Mode		X	
Console Port		X	Access through Web-based connection only
Detachable Antenna(s)	X		802.11g/b radio has detachable antenna using reverse SMA connector, for antenna replacements provided by Gateway. 802.11a does not allow detachable antennas.
Wi-Fi compliance	X		Certified March 2004
Repeater functionality	X		
Bridge functionality	X		
Internal Bridging functionality	X		Supports traffic between 802.11a/b/g clients associated on same AP
Support for Power Over Ethernet	X		LAN 1 Port using Standard 802.11I Power Injector.
LEDs	X		Power, LAN, WLAN (80211a, 80211g)
DHCP Server		X	Client only
DHCP Client	X		Client only
Static IP addressing	X		Default Static IP 192.168.1.1
802.11g	X		
802.11b	X		
802.11a	X		
802.3	X		Auto-sensing
802.3u	X		Auto-sensing
Security	X		802.1x, WPA, Wi-Fi Protected Access (64bit, 128bit WEP w/TKIP, MIC, IV Extensions, Shared Key Authentications. Supports Advanced Encryption Standard (AES)
Wireless Operating Range (indoor)	X		328 feet (100 meters)
Wireless Operating Range (outdoor)	X		1312 feet (400 meters)

Gateway	Yes	No	Comments
Wireless data rates with Automatic Fallback	X		54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, 11 Mbps, 9 Mbps, 6 Mbps, 5.5 Mbps, 2 Mbps, 1 Mbps
External Antenna Type	X		Single Detachable Dipole
Wireless Frequency Range	X		802.11b&g LAN uses 2.4000-2.4825 GHz band, 802.11a LAN uses 5.150-5.350 & 5.725-5.825 GHz bands
Modulation Technology	X		Orthogonal Frequency Division Multiplexing (OFDM), PBCC, Complementary Code Keying (CCK)
Media Access Control	X		CSMA/CA with ACK
Wireless Transmit Power	X		15dBm (32mW) +/- 2dB
Power Adapter	X		Ext. Power Supply DC 5V, 3.0A @ 100-240V ~ 50-60 Hz
Receiver Sensitivity	X		54Mbps OFDM, 10% PER, -73dBm
	X		48Mbps OFDM, 10% PER, -76dBm
	X		36Mbps OFDM, 10% PER, -82dBm
	X		24Mbps OFDM, 10% PER, -85dBm
	X		12Mbps OFDM, 10% PER, -88dBm
	X		11Mbps CCK, 8% PER, -91dBm
	X		9 Mbps OFDM, 10% PER, -90dBm
	X		6 Mbps OFDM 10% PER, -91dBm
	X		5.5 Mbps CCK, 8% PER, -92dBm
	X		2 Mbps QPSK, 8% PER, -93dBm
	X		1 Mbps BPSK, 8% PER, -94dBm
Adjustable Antenna Power	X		Full, 3/4, 1/2, 1/4 power adjustments (web based)
7x24 technical support	X		
Online support	X		
Safety and Emissions:	X		FCC, UL
Easy Installation Wizard	X		
SNMP	X		

Gateway	Yes	No	Comments
TFTP capable		X	None
802.1q VLAN capable	X		
Multiple SSID per radio	X		Supports different SSID for 802.11a & 802.11b/g
SSID Broadcast Enable/Disable	X		Per RF Radio
MAC Filtering	X		Support for Allow or Deny Listing.
Radio Enable/Disable	X		Per RF Radio
Turbo Mode	X		Increases data rates to 72Mbps (802.11A only)
Selectable/Changeable Options	X		Beacon Interval, DTIM Interval, Fragmentation Length, RTS Length, Transmit Power, Channel Selection

Appendix C

Safety, Regulatory, and Legal Information

Important safety information

Your Gateway access point is designed and tested to meet the latest standards for safety of information technology equipment. However, to ensure safe use of this product, it is important that the safety instructions marked on the product and in the documentation are followed.

Warning

Always follow these instructions to help guard against personal injury and damage to your Gateway access point.

Setting up your access point

- Read and follow all instructions marked on the product and in the documentation before you operate your access point. Retain all safety and operating instructions for future use.
- Do not use this product near water or a heat source such as a radiator.
- Install the access point on a stable work surface in an open area away from people.
- The product should be operated only from the type of power source indicated on the rating label.
- If your access point has a voltage selector switch, make sure that the switch is in the correct position for your geographic area. The power supply should be set at the factory to the correct voltage, but check to avoid possible damage.
- Openings in the case are provided for ventilation. Do not block or cover these openings. Make sure you provide adequate space, at least 6 inches (15 cm), around the AP for ventilation when you set it up. Never insert objects of any kind into the ventilation openings.
- Some products are equipped with a three-wire power cord to make sure that the product is correctly grounded when in use. The plug on this cord will fit only into a grounding-type outlet. This is a safety feature. If you are unable to insert the plug into an outlet, contact an electrician to install the appropriate outlet.
- If you use an extension cord with this access point, make sure that the total ampere rating on the products plugged into the extension cord does not exceed the extension cord ampere rating.

Warning

High voltages can enter your AP through both the power cord and the cable connections going outside the building. Protect your equipment by using a surge protector. During an electrical storm, unplug the surge protector and any cables going outside the building.

Important

A qualified electrician must perform all mains connections to power and to safety grounds. All electrical wiring must comply with applicable local or national codes and practices.

Warning

Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

Preventing static electricity discharge

The components inside your AP are extremely sensitive to static electricity, also known as *electrostatic discharge* (ESD).

Warning

To prevent risk of electric shock, do not insert any object into the vent holes of the power supply.

Caution

ESD can permanently damage electrostatic discharge-sensitive components in your AP.

Care during use

- Do not walk on the power cord or allow anything to rest on it.
- Do not spill anything on the access point. The best way to avoid spills is to avoid eating and drinking near your access point.
- Some products have a replaceable CMOS battery on the system board. There is a danger of explosion if the CMOS battery is replaced incorrectly. Replace the battery with the same or equivalent type recommended by the manufacturer. Dispose of batteries according to the manufacturer's instructions.
- When an AP is turned off, a small amount of electrical current still flows through it. To avoid electrical shock, always unplug all cables from the device (power, modem and network cables are some examples), before cleaning the access point.
- Unplug the access point from the wall outlet and refer servicing to qualified personnel if:
- The power cord or plug is damaged.
- Liquid has been spilled into the access point
- The access point does not operate correctly when the operating instructions are followed.
- The access point was dropped or the case is damaged.
- The access point operation changes.

Important

Do not use Gateway products in areas classified as hazardous locations. Such areas include patient care areas of medical and dental facilities, oxygen-laden environments, or industrial facilities.

Regulatory compliance statements

Wireless Guidance

The Gateway 7001 Series APs, (low power Radio Frequency, RF, transmitting device), operate in the 2400-2483.5 MHz band for 802.11B&G and 5 GHz bands for 802.11A. The following section is a general overview of considerations while operating the wireless LAN.

Limitations, cautions, and concerns are listed below and in the specific country sections (or country group sections). This wireless device is only qualified for use in the countries identified by the Radio Approval Marks on the device rating label. If the country you will be using the wireless device in is not listed, please contact that countries local Radio Approval agency for requirements prior to operation. Wireless devices are closely regulated and use may not be allowed.

The power output of the device is well below the RF exposure limits as known at this time. Because this wireless device emits less energy than is allowed in radio frequency safety standards and recommendations, Gateway believes these devices are safe for use. Regardless of the power levels, care should be taken to minimize human contact during normal operation.

Measurements have been performed to show that the RF exposure is below what is considered safe limits; however care should be taken to make sure the user or bystanders keep the transmitter away from their body when the wireless device is transmitting. The transmitting antenna should be installed and used in a manner to maintain 20cm (8 inches) from user's or bystander's bodies.

This wireless device is intended to be used indoors. In some areas, use of this device outdoors is prohibited.

Some circumstances require restrictions on using wireless devices. Examples of common restrictions are listed below:

Warning

In environments where the risk of interference to other devices or services is harmful or perceived as harmful, the option to use a wireless device may be restricted or eliminated. Airports, Hospitals, and Oxygen or flammable gas laden atmospheres are limited examples where use of wireless devices may be restricted or eliminated. When in environments where you are uncertain of the sanction to use wireless devices, ask the applicable authority for authorization prior to use or turning on the wireless device.

Warning

Do not operate the wireless device unless all covers and shields are in place and the system is fully assembled.

Warning

Wireless devices are not user serviceable. Do not modify them in any way. Modification to a wireless device will void the authorization to use it. Please contact Gateway for service.

Warning

Only use drivers or firmware approved for the country in which the device will be used. See the Gateway System Restoration Kit, or contact Gateway Technical Support for additional information.

United States of America

Federal Communications Commission (FCC) Intentional emitter per FCC Part 15

The power output of the AP is well below the RF exposure limits as known at this time. Because this wireless device emits less energy than is allowed in radio frequency safety standards and recommendations, Gateway believes these devices are safe for use.

Regardless of the power levels, care should be taken to minimize human contact during normal operation.

Measurements have been performed to show that the RF exposure is below what is considered safe limits; however care should be taken to make sure the user or bystanders keep the transmitter away from their body when the wireless device is transmitting. The transmitting antenna should be installed and used in a manner to maintain 20cm (8 inches) from user's or bystander's bodies.

This wireless device is intended to be used indoors. In some areas, use of this device outdoors is prohibited.

Operation of this device is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation of the device.

Warning

In order to comply with FCC requirements this transmitter must not be operated (or co-located) in conjunction with any other transmitter or antenna.

Warning

Wireless devices are not user serviceable. Do not modify them in any way. Modification to a wireless device will void the authorization to use it. Please contact Gateway for service.

Unintentional emitter per FCC Part 15

This device has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio or television reception. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause interference to radio and television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help.

Compliance Accessories: These accessories are required to be used in order to ensure compliance with FCC rules: The AC Adapter supplied with the device.

Wireless Channels: Gateway declares that the Gateway 7001 802.11 A+G Wireless Access Point is limited to channels 1 through 11, specified by firmware controlled in the USA.

FCC declaration of conformity

Responsible party:

Gateway Companies, Inc.
610 Gateway Drive, North Sioux City, SD 57049
(605) 232-2000 Fax: (605) 232-2023

Products:

- Gateway 7001 AP

For unique identification of the product configuration, please submit the 10-digit serial number found on the product to the responsible party.

This device complies with Part 15 of the FCC Rules. Operation of this product is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Caution

Changes or modifications not expressly approved by Gateway could void the FCC compliance and negate your authority to operate the product.

Notices

14303 Gateway Place
Poway, CA 92064 USA

All Rights Reserved

The information in this manual has been carefully checked and is believed to be accurate. However, changes are made periodically. These changes are incorporated in newer publication editions. Gateway may improve and/or change products described in this publication at any time. Due to continuing system improvements, Gateway is not responsible for inaccurate information which may appear in this manual. For the latest product updates, consult the Gateway Web site at www.gateway.com. In no event will Gateway be liable for direct, indirect, special, exemplary, incidental, or consequential damages resulting from any defect or omission in this manual, even if advised of the possibility of such damages.

In the interest of continued product development, Gateway reserves the right to make improvements in this manual and the products it describes at any time, without notices or obligation.

Trademark Acknowledgments

Gateway and the Black-and-White Spot Design are trademarks or registered trademarks of Gateway, Inc. in the U.S. and other countries. SpotShop, Spotshop.com, and Your:)Ware are trademarks of Gateway, Inc. Intel, Intel Inside logo, and Pentium are registered trademarks and MMX is a trademark of Intel Corporation. Microsoft, MS, MS-DOS, and Windows are trademarks or registered trademarks of Microsoft Corporation. Instant802 Networks and the Instant802 Networks logo are trademarks of Instant802 Networks, Inc. and/or its affiliates in the US and other countries. All other product names mentioned herein are used for identification purposes only, and may be the trademarks or registered trademarks of their respective companies.

Third Party Copyright Acknowledgements

CGL Library source code: Copyright © 1998-2000 Carson S.K. Harding. Mini-httpd source code: Copyright © 1999,2000 by Jef Poskanzer <jef@acme.com>. This product includes software developed by the University of California, Berkeley and its contributors.Specifically, local_passwd.c source code: Copyright © 1990, 1993, 1994 Regents of University of California. Full copyright acknowledgements for third party software is available in a separate readme file accompanying the product.

Macrovision statement

If your computer has a DVD drive and an analog TV Out port, the following paragraph applies:

This product incorporates copyright protection technology that is protected by method claims of certain U.S. patents and other intellectual property rights owned by Macrovision Corporation and other rights owners. Use of this copyright protection technology must be authorized by Macrovision Corporation, and is intended for home and other limited viewing uses only unless otherwise authorized by Macrovision Corporation. Reverse engineering or disassembly is prohibited.

Index

V

W

A MAN 7001 SRS ACC PTS GDE R1 05/04

8 27103 03761 6

8510029